

Table of Contents

Chapter 1

Introduction.....	1
Huang Dao Pei	3
Peter H. Lee—Update.....	3
The Cox Report.....	4
Commercial and Intelligence Operations: PRC Acquisition of US Technology	5
The 863 and Super-863 Programs: Importing Technologies for Military Use	5
The PRC’s Use of Intelligence Services To Acquire US Military Technology	7
The “Pricelings”	7
Acquisition of Military Technology From the United States	9
Joint Ventures With US Companies	10
Acquisition and Exploitation of Dual-Use Technologies	11
Front Companies.....	13
Direct Collection of Technology by Non-Intelligence Agencies and Individuals	14
Illegal Export of Military Technology Purchased in the United States	18
PRC Purchase of Interests in US Companies	19
Methods Used by the PRC to Export Military Technology From the United States	21
PRC Incentives for US Companies To Advocate Relaxation of Export Controls	22
PRC Theft of US Thermonuclear Warhead Design Information	23
How the PRC Acquired Thermonuclear Warhead Design Information From the United States: PRC Espionage and Other PRC Techniques	24
How the US Government Learned of the PRC’s Theft of Our Most Advanced Thermonuclear Warhead Design Information	25
The “Walk-In”.....	25
US Government Investigations of Nuclear Weapons Design Information Losses	26
Investigation of Theft of Design Information for the W-88 Trident D-5 Thermonuclear Warhead	27
Investigation of Additional Incidents	27
The Department of Energy’s Counterintelligence Program at the US National Weapons Laboratories	28
PRC Gains Sensitive Information From Hughes	29
LORAL Investigation of Intelsat Launch Failure Provides PRC With Sensitive Information	31
PRC Targeting of Advanced Machine Tools.....	33
Case Study: McDonnell Douglas Machine Tools.....	33
PRC Targeting of US Jet Engines and Production Technology	34
Case Study: Garrett Engines.....	36
PRC Targeting of Garrett Engines	36
US Government Approval of the Initial Garrett Engine Exports	37
Commerce Department Decontrol of the Garrett Jet Engines	37
The Interagency Review of the Proposed Export of Garrett Engines.....	38
Consideration of Enhanced Proliferation Control Initiative Regulations	39
Consideration of COCOM and Export Administration Regulations	40
Resolution of the Garrett Engine Controversy	42

The PRC Continues To Acquire Jet Engine Production Processes	43
White House Response to Cox Report—1 February 1999	50
Security at US National Laboratories	50
Missile and Space Technology	51
Domestic and International Export Policies	53
High-Performance Computers	53
Chinese Technology Acquisition and Proliferation Activities	54
China’s High-Tech Espionage Textbook	54
Operational Collection	56
Open Sources	56
Conferences	57
Old-Fashioned Espionage	58
Report on the Investigation of Espionage Allegations Against Dr. Wen Ho Lee—8 March 2000	58
Summary	58
The Investigation of 1982-84	59
The Investigation of Dr. Lee From 1994 to 2 November 1995	60
The Investigation Renewed—30 May 1996 to 12 August 1997	61
Investigation From 12 August 1997 to 23 December 1998	69
DOE’s Interference in the Investigation	70
10 February 1999 to 8 March 1999	71
8 March 1999 to 7 April 1999	72
Reopening the W-88 Investigation and the Criminal Case Against Dr. Lee	72
David Tzu Wvi Yang and Eugene You Tsai Hsu	77
Public Announcement—US Department of State—Office of the Spokesman	78

Chapter 2

Introduction	79
Theodore Alvin Hall	81
State Department Security Breaches	81
David Sheldon Boone	83
Daniel King Case	89
Stanislav Gusev	93
George Trofimoff	93
George Trofimoff Affidavit	95
Robert Philip Hanssen	102
Hanssen’s FBI Career	106
Letters to the KGB/SVR	107
Letters From the KGB/SVR	114
Newspaper Ads/Telephone Calls	116
Deaddrops	117
Escrow Account in Moscow	128
The End Game	129

Russian Counterintelligence Begins Comeback	132
Introduction	132
Yeltsin Begins CI Reorganization	132
Barsukov Takes FSB's Reins	133
Protection of State Secrets Upgraded	136
Other Security Services Changes	140
FSB Comes Out on Top	140
Yeltsin Fires FSB and SBP Chiefs	141
Media Plays Up Arrests	144
Influences on Yeltsin's Decision	144
Reformers' Versions	145
Kovalev Named FSB Chief	146
Kovalev Out—Putin In	148
Under President Putin: FSB Supplants the "Old Guard"	149
Putin's Second Year	149
Changes in the FSB	153
Returning to Yesteryear	154
FSB and the Media	154
The Roots of Putin's Attack on Media Freedom	156
FSB Legalizes Monitoring of Internet	157
Crackdown on Russian Scientists	157
FSB Takes Charge of Chechen Operations	158
Celebrating Chekist Day Again	158
Public Perception of the FSB	159
Putin: A Reflection of Andropov	159
Specific Cases	159
Targeting Humanitarian Groups	177
Foreign Intelligence	177
Russian Spies Caught	178
Poland Arrests Russian Spies	179
Poland Expels Russians	179
Reaction to US Expulsion of Russian Diplomats	179
Russian Defections	180
The GRU	180
Vladimir Semichastny	185
Ruth Werner	186
Chapter 3	
Introduction	187
Kai-Lo Hsu, Chester S. Ho, and Jessica Chou	188
Theresa Squillacote, Kurt Stand, and James Clark: The Espionage Careers of Three Americans	189
French SIGINT Targeting	202

Updates on Two Espionage Cases	204
Douglas F. Groat	204
Robert Kim	204
Cuban Spies in Miami.	206
Geraldo Hernandez	207
Ramon Labanino	208
Antonio Guerrero	209
Alejandro Alonso	209
Rene Gonzalez	210
Nilo Hernandez and Linda Hernandez	210
Fernando Gonzalez	212
Joseph Santos and Amarylis Silverio	212
Five Ring Members Get Plea Bargains	213
Cuba Gets Christmas Gift From the United States	213
The Remaining Five Members Tried and Convicted	213
Brian P. Regan	215
Avery Dennison.	218
Kelly Therese Warren	229
Jean-Philippe Wispelaere	231
Mariano Faget	232
Echelon	235
The Operations of Foreign Intelligence Services	238
The Operations of Certain Intelligence Services	240
Technical Conditions Governing the Interception of Telecommunications	242
The Example of the German Federal Intelligence Service	245
Satellite Communications Technology	246
The Most Important Satellite Communication Systems	248
Regional Satellite Systems	249
National Satellite Systems	250
The Allocation of Frequencies	250
Satellite Communications for Military Purposes	251
Clues to the Existence of at Least One Global Interception System	252
How Can a Satellite Communications Interception Station be Recognized?	253
Publicly Accessible Data About Known Interception Stations	254
The Stations in Detail	255
Further Stations	257
The UKUSA Agreement	259
Powers of the Intelligence Agencies	261
Information From Authors and Journalists	261
Information From Government Sources	265
Parliamentary Reports	266

Might There be Other Global Interception Systems?	267
Compatibility of an ECHELON Type Communications Interception System With Union Law	268
The Compatibility of Communications Surveillance by Intelligence Services With the Fundamental Right to Privacy	270
Protection Against Industrial Espionage	279
Intelligence Services	281
Legal Situation With Regard to the Payment of Bribes to Public Officials	291
Security of Computer Networks	293
Cryptography as a Means of Self-Protection	297
The EU's External Relations and Intelligence Gathering	302
Conclusions and Recommendations	304
Recommendations	307
George and Marisol Gari	320
Japan	322
The South Korean National Intelligence Service	326
Background	326
The Creation of the Korean Central Intelligence Agency	328
Agency for National Security Planning	329
Government and Private-Sector Efforts To Steal US Technological Secrets	332
South Korea's Informal Technology Acquisitions	334
Cooperation Centers To Acquire Technologies	336
Science Ministry Continues Foreign Recruitment Drive	337
Technology-Transfer Facility in San Diego	337

Chapter 4

Introduction	341
The Rudman Report	343
Foreword From the Special Investigative Panel	343
Prospects for Reforms	344
Solutions	345
Bottom Line	346
Findings	346
Root Causes	350
Big, Byzantine, and Bewildering Bureaucracy	350
Lack of Accountability	351
Culture and Attitudes	352
Changing Times, Changing Missions	352
Recurring Vulnerabilities	352
Management and Planning	353
Physical Security	356
Screening and Monitoring of Personnel	357

Protection of Classified and Sensitive Information.	358
Foreign Visitors and Assignments Program	359
Responsibility	360
The Record of the Clinton Team.	361
The 1995 “Walk-In” Document	362
W-88 Investigation	362
PFIAB Evaluation of the Intelligence Community Damage Assessment.	363
Presidential Decision Directive 61: Birth and Intent	363
Timeliness of PDD-61	365
Secretary Richardson’s Initiatives.	365
Prospects for Reforms.	367
Trouble Ahead.	367
Security and Counterintelligence Accountability	368
Personnel Security	368
Physical/Technical/Cyber Security	368
Business Issues	369
Intelligence Community Damage Assessment of China’s Acquisition of US Nuclear Weapons Information	369
Central Intelligence Agency Inspector General Report of Investigation—John M. Deutch.	372
Aftermath of the IG Report.	410
DOE Counterintelligence Failures	414
Report of the Redmond Panel.	414
Leaks	427
Timothy Steven Smith.	429
Waguespack Leaves NACIC.	430
Jolene Hilda Neat Rector and Steven Michael Snyder	430
Takashi Okamoto and Hiroaki Serizawa.	432
Ana Belen Montes.	434
Communication From the Cuban Intelligence Service (CuIS) to Montes via Shortwave Radio	434
Communication Between the CuIS and Montes via Computer Diskette	435
Communication From Montes to the CuIS by Pager	435
Montes’s Transmission of Classified Information to the CuIS	436
FBI Physical Surveillance of Montes and Telephone Records for May to September 2001	437
The Threat to Laptop Computers	439
The Presidential Decision Directive on CI-21: Counterintelligence for the 21st Century	443
National Security Presidential Directive-1	446
Bibliography Volume IV.	451
CI Calendar of Events.	455

CHAPTER 1

INTRODUCTION

In 1978, a series of unofficial exchange visits between US nuclear weapons experts and their People's Republic of China (PRC) counterparts began. The PRC officials made a serious concentrated effort to cultivate close relationships with certain US experts. Over the subsequent 23 years, as a result of this exchange, the PRC made major strides in the development of nuclear weapons, including the neutron bomb.

Beginning in 1998, US media sources began reporting about ongoing investigations of four cases of suspected Chinese espionage against the United States dating back to the 1980s. The most serious case involved China's alleged acquisition of key information about our nation's most advanced miniaturized US nuclear warhead, the W-88, as well as serious security breaches at the Department of Energy's (DOE) Los Alamos Laboratory between 1984 and 1988.

Early in 1998, Congressional focus turned to US satellite exports to China. A US Department of Defense classified report concluded that scientists from Hughes and Loral Space and Communications, involved in studying the 1996 crash of a Chinese rocket launching a Loral satellite, provided scientific expertise to China that notably improved the reliability of China's missile launch abilities.

After this information was published in the US media, a special House Select Committee and a number of Senate committees investigated US technology transfer policy with respect to China. The result was the release of the Report of the Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China (the Cox Report). The report dealt, among other things, with the possible compromise of highly classified information on DOE's nuclear weapons laboratories.

After the release of the Cox Report, President William Clinton requested the President's Foreign Intelligence Advisory Board (PFIAB), chaired by former Senator Walter Rudman, to review the security threat at DOE's nuclear weapons laboratories and the measures taken to address that threat. In June 1999, the PFIAB presented its report to the President. The report found that DOE "is a dysfunctional bureaucracy that has proven it is incapable of reforming itself."

In 1999, the press reported about an investigation by the FBI against a Taiwan-born Chinese American scientist, Wen Ho Lee, who downloaded critical nuclear weapons codes, called legacy codes, from a classified computer system at Los Alamos to an unclassified system accessible by anyone with the proper password. Suspected of espionage, Wen Ho Lee was charged with only one count of mishandling national security information to which he pled guilty and sentenced to time served. The FBI came under heavy criticism that it mishandled the investigation and exaggerated the case against Lee.

Congressional concern over security at the nuclear weapons laboratories increased again in June 2000 when it was discovered that computer hard drives containing nuclear weapons information disappeared at Los Alamos. The drives later turned up, and a FBI investigation of the missing failed to determine who took them.

A major crisis between China and the United States occurred when a US Navy EP-3 reconnaissance aircraft, conducting a routine and solo reconnaissance mission approximately 50 to 60 miles off the Chinese coast, collided with a Chinese jet fighter on 1 April 2001. The Chinese fighter crashed, and the pilot died. The US Navy plane made an emergency landing at a military base on China's Hainan Island. The Chinese held the Navy

crew for 11 days and released them only when the US Ambassador delivered a letter of regret over the intrusion of China's airspace and landing without verbal clearance from the Chinese.

In 1999, the American press began to publish articles that stated the Chinese Government was arresting prominent activists and handing out harsh jail sentences for reasonable civil liberties. On 15 August 1999 two independent researchers, one of whom was an American, were arrested for conducting interviews about a pending World Bank project. During an interrogation by Chinese security officials, the American was seriously injured when he jumped out of a third story window.

In early 2000, Chinese authorities initiated a major crackdown against overseas Chinese visitors, some of whom had US connections. They arrested eight American citizens or permanent residents of the United States. The arrests clouded bilateral relations between the United States and China and were raised at the highest political level. Several were subsequently tried, convicted, and allowed to leave China.

Chinese intelligence, like those of other countries in the post-Cold War era, has increasingly focused on economic, industrial, commercial, and technological information. There have been reports of Chinese companies in the United States being connected to China's military industrial complex through which American technologies are allegedly being transferred back to China. In addition, corporate espionage and illegal transfer of American technology will increase as the United States and China expands their relationship both politically and commercially.

Huang Dao Pei

The FBI arrested Huang Dao Pei, a Chinese-born naturalized US citizen living in Piscataway, New Jersey, on 28 July 1998 on charges he tried to steal trade secrets for a hepatitis C monitoring kit he hoped to sell in China. Huang, a former scientist who worked at Roche Diagnostics from 1992 to 1995, allegedly tried to buy information from a scientist who worked for Roche. The scientist was cooperating with the FBI.

According to court papers, Huang telephoned the cooperating scientist on two occasions asking for specific documents that would help him duplicate parts of the kit. Huang promised to pay the scientist for the risk involved in obtaining the documents. He told the scientist he needed the information so his firm, LCC Enterprises, could develop a similar kit and sell it in China.

As reported in the open press, the FBI declined to say whether Huang was working for the Chinese, but it was noted that China is among the most aggressive countries going after US trade secrets. A Roche representative stated that, if a competitor were to obtain the information sought by Huang, it could avoid spending the millions of dollars and years that Roche spent developing the product.

Peter H. Lee—Update¹

On 26 March 1998, Dr. Peter S. Lee, the nuclear physicist convicted of two felony counts including passing classified national defense information to PRC representatives, was sentenced to spend one year in a community corrections facility. In addition to the one-year term, he was ordered to serve three years of probation, perform 3,000 hours of community service, and pay \$20,000 in fines.

In a case apparently involving empathy instead of greed, Lee admitted under a plea bargain agreement on 7 December 1997, that he passed classified defense secrets to the Chinese Government in 1985 while working as a research physicist at Los Alamos National Laboratory. Lee, a naturalized US citizen who was born in Taiwan, was working on classified projects relating to the use of lasers to simulate nuclear detonations. The information was declassified in the early 1990s. He was fired by TRW on the same day he pleaded guilty.

Lee passed the classified information in 1985 while he was doing research at the Los Alamos National Laboratory in New Mexico. Lee had traveled to China where he was asked by a Chinese scientist to discuss the construction of hohlraums, a diagnostic device used in conjunction with lasers to create microscopic nuclear detonations. The day after he initially revealed the classified information, Lee gave a lecture to about 30 Chinese nuclear scientists in which he again gave away secret restricted data regarding the manufacture and use of hohlraums. Lee told the FBI that he disclosed the information because he wanted to help his Chinese counterparts, and he wanted to enhance his reputation there.

The second charge against Lee concerns disclosures he failed to make in 1997 while he was working on classified research projects for TRW. Before he traveled to China on vacation, Lee was required to fill out a security form in which he stated that he would not be giving lectures on his work during his trip. Upon his return, he had to fill out a second form in which he confirmed that he did not give any lectures of a technical nature.

However, as Lee later confessed to the FBI, he lied on both forms because he intended to and did, in fact, deliver lectures to Chinese scientists that discussed his work at TRW.

Endnote

¹ For previous information on Peter Lee, see *Counterintelligence Reader*, Volume III, p. 410.

The Cox Report

(Editor's Note: This edited version of the report written by the Select Committee on U.S. National Security and Military/Commercial Concerns with The People's Republic of China [referred to as the Cox Committee] is printed verbatim. This edited version of the Committee's report [known as the Cox Report] concentrates on China's collection methodologies in obtaining US technology and the US investigation of those methodologies.)

It is extremely difficult to meet the challenge of the PRC's technology acquisition efforts in the United States with traditional counterintelligence techniques that were applied to the Soviet Union. Whereas Russians were severely restricted in their ability to enter the United States or to travel within it, visiting PRC nationals, most of whom, come to pursue lawful objectives, are not so restricted. Yet the PRC employs all types of people, organizations, and collection operations to acquire sensitive technology: threats to national security can come from PRC scientists, students, business people, or bureaucrats, in addition to professional civilian and military intelligence operations.

The PRC is striving to acquire advanced technology of any sort, whether for military or civilian purposes, as part of its program to improve its entire economic infrastructure.¹ This broad targeting permits the effective use of a wide variety of means to access technology. In addition, the PRC's diffuse and multi-pronged technology-acquisition effort presents unique difficulties for US intelligence and law enforcement agencies, because the same set of mechanisms and organizations used to collect technology in general can be used, and are used to collect military technology.

In light of the number of interactions taking place between PRC and US citizens and organizations over the last decade as trade and other forms of cooperation have bloomed, the opportunities for the PRC to attempt to acquire information and technology, including sensitive national security secrets, are immense. Moreover, the PRC often

does not rely on centralized control or coordination in its technology acquisition efforts, rendering traditional law enforcement, intelligence, and counterintelligence approaches inadequate. While it is certainly true that not all of the PRC's technology acquisition efforts are a threat to US national security, that very fact makes it quite a challenge to identify those that are.

The PRC's blending of intelligence and non-intelligence assets and reliance on different collection methods presents challenges to US agencies in meeting the threat. In short, as James Lilley, former US Ambassador to the PRC says, US agencies are "going nuts" trying to find MSS and MID links to the PRC's military science and technology collection, when such links are buried beneath layers of bureaucracy or do not exist at all.²

Commercial and intelligence operations: PRC acquisition of US technology

The State Council controls the PRC's military-industrial organizations through the State Commission of Science, Technology and Industry for National Defense (COSTIND). Created in 1982, COSTIND was originally intended to eliminate conflicts between the military research and development sector and the military production sector by combining them under one organization. Soon its role broadened to include the integration of civilian research, development, and production efforts into the military.

COSTIND presides over a vast, interlocking network of institutions dedicated to the specification, appraisal, and application of advanced technologies to the PRC's military aims. The largest of these institutions are styled as corporations, notwithstanding that they are directly in service of the Chinese Communist Party (CCP), the PLA, and the State. They are:

- China Aerospace Corporation (CASC)
- China National Nuclear Corporation (CNNC)
- China North Industries Group (NORINCO)

- Aviation Industries Corporation of China (AVIC)
- China State Shipbuilding Corporation (CSSC)

Until 1998, COSTIND was controlled directly by both the Central Military Commission and the State Council. In March 1998, COSTIND was "civilianized" and now reports solely to the State Council. A new entity, the General Armament Department (GAD), was simultaneously created under the CMC to assume responsibility for weapons system management and research and development.

The 863 and Super-863 Programs: Importing Technologies for Military Use

In 1986, "Paramount Leader" Deng Xiaoping³ adopted a major initiative, the so-called 863 Program, to accelerate the acquisition and development of science and technology in the PRC.⁴ Deng directed 200 scientists to develop science and technology goals. The PRC claims that the 863 Program produced nearly 1,500 research achievements by 1996 and was supported by nearly 30,000 scientific and technical personnel who worked to advance the PRC's "economy and . . . national defense construction."⁵

The most senior engineers behind the 863 Program were involved in strategic military programs such as space tracking, nuclear energy, and satellites.⁶ Placed under COSTIND's management, the 863 Program aimed to narrow the gap between the PRC and the West by the year 2000 in key science and technology sectors, including the military technology areas of:

- Astronautics
- Information technology
- Laser technology
- Automation technology
- Energy technology
- New materials

The 863 Program was given a budget split between military and civilian projects, and focuses on both

military and civilian science and technology. The following are key areas of military concern:

- **Biological Warfare:** The 863 Program includes a recently unveiled plan for gene research that could have biological warfare applications.
- **Space Technology:** Recent PRC planning has focused on the development of satellites with remote sensing capabilities, which could be used for military reconnaissance, as well as space launch vehicles.
- **Military Information Technology:** The 863 Program includes the development of intelligent computers, optoelectronics, and image processing for weather forecasting; and the production of submicron integrated circuits on 8-inch silicon wafers. These programs could lead to the development of military communications systems; command, control, communications, and intelligence systems; and advances in military software development.
- **Laser Weapons:** The 863 Program includes the development of pulse-power techniques, plasma technology, and laser spectroscopy, all of which are useful in the development of laser weapons.
- **Automation Technology:** This area of the 863 Program, which includes the development of computer-integrated manufacturing systems and robotics for increased production capability, is focused in the areas of electronics, machinery, space, chemistry, and telecommunications, and could standardize and improve the PRC's military production.
- **Nuclear Weapons:** Qinghua University Nuclear Research Institute has claimed success in the development of high-temperature, gas-cooled reactors, projects that could aid in the development of nuclear weapons.
- **Exotic Materials:** The 863 Program areas include optoelectronic information materials, structural materials, special function materials,

composites, rare-earth metals, new energy compound materials, and high-capacity engineering plastics. These projects could advance the PRC's development of materials, such as composites, for military aircraft and other weapons.

In 1996, the PRC announced the "Super 863 Program" as a follow-on to the 863 Program, planning technology development through 2010. The "Super 863 Program" continues the research agenda of the 863 Program, which apparently failed to meet the CCP's expectations.

The Super 863 Program calls for continued acquisition and development of technology in a number of areas of military concern, including machine tools, electronics, petrochemicals, electronic information, bioengineering, exotic materials, nuclear research, aviation, space, and marine technology.

COSTIND and the Ministry of Science and Technology jointly manage the Super 863 Program. The Ministry of Science and Technology focuses on biotechnology, information technology, automation, nuclear research, and exotic materials, while COSTIND oversees the laser and space technology fields.⁷

COSTIND is attempting to monitor foreign technologies, including all those imported into the PRC through joint ventures with the United States and other Western countries. These efforts are evidence that the PRC engages in extensive oversight of imported dual-use technology. The PRC is also working to translate foreign technical data, analyze it, and assimilate it for PLA military programs. The Select Committee has concluded that these efforts have targeted the US Government and other entities.

If successful, the 863 Programs will increase the PRC's ability to understand, assimilate, and transfer imported civil technologies to military programs. Moreover, Super 863 Program initiatives increasingly focus on the development

of technologies for military applications. PRC program managers are now emphasizing projects that will attract US researchers.

Since the early 1990s, the PRC has been increasingly focused on acquiring US and foreign technology and equipment, including particularly dual-use technologies that can be integrated into the PRC's military and industrial bases.

The PRC's Use of Intelligence Services To Acquire US Military Technology

The primary professional PRC intelligence services involved in technology acquisition are the Ministry of State Security (MSS) and the PLA General Staff's Military Intelligence Department (MID).

In addition to and separate from these services, the PRC maintains a growing non-professional technology-collection effort by other PRC Government-controlled interests, such as research institutes and PRC military-industrial companies. Many of the most egregious losses of US technology have resulted not from professional operations under the control or direction of the MSS or MID, but as part of commercial, scientific, and academic interactions between the United States and the PRC.

Professional intelligence collectors, from the MSS and MID, account for a relatively small share of the PRC's foreign science and technology collection. Various non-professionals, including PRC students, scientists, researchers, and other visitors to the West, gather the bulk of such information. These individuals sometimes are working at the behest of the MSS or MID, but often represent other PRC-controlled research organizations - scientific bureaus, commissions, research institutes, and enterprises.

Those unfamiliar with the PRC's intelligence practices often conclude that, because intelligence services conduct clandestine operations, all clandestine operations are directed by intelligence agencies. In the case of the PRC, this is not always

the rule. Much of the PRC's intelligence collection is independent of MSS direction. For example, a government scientific institute may work on its own to acquire information.

Minister Xu Yongyue, a member of the CCP Central Committee, heads the MSS. The MSS reports to Premier Zhu Rongji and the State Council, and its activities are ultimately overseen by the CCP Political Science and Law Commission. It is a usual practice for senior members of the CCP's top leadership to be interested in the planning of PRC military acquisitions.

The MSS conducts science and technology collection as part of the PRC's overall efforts in this area. These MSS efforts most often support the goals of specific PRC technology acquisition programs, but the MSS will take advantage of any opportunity to acquire military technology that presents itself.

The MSS relies on a network of non-professional individuals and organizations acting outside the direct control of the intelligence services, including scientific delegations and PRC nationals working abroad, to collect the vast majority of the information it seeks.

The PLA's MID, also known as the Second Department of the PLA General Staff, is responsible for military intelligence. PLA General Ji Shengde, the son of a former PRC Foreign Minister, currently runs it. One of the MID's substantial roles is military-related science and technology collection.

The 'Princelings'

Unlike the Soviet Union, where nepotism in the Communist Party was rare, ruling in the PRC is a family business. Relatives of the founders of the Chinese Communist Party rise quickly through the ranks and assume powerful positions in the CCP, the State, the PLA, or the business sector. These leaders, who owe their positions more to family

connections than to their own merit, are widely known as “princelings.”⁸

Political, military, and business leaders in the PRC exercise considerable influence within their respective hierarchies. With the exception of those who make their way to the uppermost levels of the CCP or State bureaucracies, however, their authority, power, and influence extend only to those below them within that hierarchy. They have little ability to influence either the leaders above them within their own hierarchy or the leaders in other hierarchies.⁹

Princelings operate outside these structures. Because of their family ties and personal connections to other CCP, PLA, and State officials, they are able to “cross the lines” and accomplish things that might not otherwise be possible.¹⁰

The Cox Committee identified two as most notable princelings, Wang Jun and Liu Chaoying, which the Committee said had been directly involved in illegal activities in the United States.

Wang Jun is the son of the late PRC President Wang Zhen. At the time, Wang simultaneously held two powerful positions in the PRC. He was Chairman of the China International Trade and Investment Company (CITIC), the most powerful and visible corporate conglomerate in the PRC. He was also the President of Polytechnologies Corporation, an arms-trading company and the largest and most profitable of the corporate structures owned by the PLA. Wang’s position gave him considerable clout in the business, political, and military hierarchies in the PRC.¹¹

Wang was publicly known in the United States for his role in the 1996 campaign finance scandal and for Polytechnologies’ indictment stemming from its 1996 attempt to smuggle 2,000 Chinese AK-47 assault rifles into the United States. He attended a White House “coffee” with President Clinton in February 1996 and met with Commerce Secretary Ronald Brown the following day. He was also connected to over \$600,000 in illegal campaign

contributions made by Charlie Trie to the US Democratic National Committee (DNC).¹²

Liu Chaoying is the daughter of former CCP Central Military Commission Vice-Chairman and Politburo Standing Committee member General Liu Huaqing, who has used numerous US companies for sensitive technology acquisitions. General Liu has been described as the PLA’s preeminent policymaker on military R&D, technology acquisition, and equipment modernization as well as the most powerful military leader in the PRC. His daughter was a Lieutenant Colonel in the PLA and has held several key and instrumental positions in the PRC’s military industry, which is involved in numerous arms transactions and international smuggling operations.¹³ On two occasions, she has entered the United States illegally and under a false identity.

Col. Liu Chaoying was then a Vice-President of China Aerospace International Holdings, a firm specializing in foreign technology and military sales.¹⁴ It is the Hong Kong subsidiary of China Aerospace Corporation, the organization that manages the PRC’s missile and space industry. Both organizations benefit from the export of missile or satellite-related technologies and components from the United States, as does China Great Wall Industry Corporation, Col. Liu’s former employer and a subsidiary of China Aerospace Corporation, which provides commercial space launch services to American satellite manufacturers.

China Aerospace Corporation is also a substantial shareholder in both the Apstar and APMT projects to import US satellites to the PRC for launch by China Great Wall Industry Corporation.¹⁵

A Chinese-American, Johnny Chung, during the course of plea negotiations, disclosed that during a trip to Hong Kong in the summer of 1996, he met with Col. Liu and the head of the MID, Gen. Ji Shengde. According to Chung, he received \$300,000 from Col. Liu and Gen. Ji as a result of this meeting. The FBI confirmed the deposit into

Chung's account from Hong Kong and that the PLA officials likely served as the conduit for the money.

The Cox Committee determined that Col. Liu's payment to Johnny Chung was an attempt to better position her in the United States to acquire computer, missile, and satellite technologies. The purpose of Col. Liu's contacts was apparently to establish reputable ties and financing for her acquisition of technology such as telecommunications and aircraft parts.¹⁶

Within one month after meeting with Col. Liu in Hong Kong, Chung formed Marswell Investment, Inc., possibly capitalizing the new company with some of the \$300,000 he had received from Col. Liu and Gen. Ji.¹⁷ Col. Liu was designated as president of the company, which was based in Torrance, California. The company is located in southern California, in the same city where China Great Wall Industry Corporation also maintains its US subsidiary.

Col. Liu made two trips to the United States, one in July 1996 and one in August 1996, apparently seeking to expand her political and commercial contacts. During Col. Liu's July trip, Chung arranged for her to attend a DNC fundraiser where she met President Clinton and executives involved in the import-export business.¹⁸ Shortly afterwards, Chung also arranged for her to meet with the Executive Vice President of the Federal Reserve Bank of New York.¹⁹

Liu's August 1996 trip to the United States came at the invitation of Chung, who had told her that he had contacted Boeing and McDonnell Douglas regarding her interest in purchasing aircraft parts.²⁰

That same month, Col. Liu traveled to Washington, D.C., where Chung had contacts arrange for her to meet with representatives of the Securities and Exchange Commission to discuss listing a PRC company on US stock exchanges.²¹ Soon after the meeting, when Chung and Liu's alleged involvement in the campaign finance scandal

became the subject of media reports, Col. Liu left the United States. Marswell remains dormant.²²

Princelings such as Wang and Liu present a unique technology transfer threat because their multiple connections enable them to move freely around the world and among the different bureaucracies in the PRC. They are therefore in a position to pull together the many resources necessary to carry out sophisticated and coordinated technology acquisition efforts.²³

Acquisition of Military Technology from the United States

The PRC has stolen military technology from the United States, but until recently, the United States has lawfully transferred little to the PLA. This has been due, in part, to the sanctions imposed by the United States in response to both the 1989 Tiananmen Square massacre and to the PRC's 1993 transfer of missile technology to Pakistan.

During the Cold War, the United States assisted the PRC in avionics modernization of its jet fighters under the US Peace Pearl program.²⁴

After the relatively "cool" period in US-PRC relations in the early 1990s, the trend since 1992 has been towards liberalization of dual-use technology transfers to the PRC.²⁵ Recent legal transfers include the sale of approximately 40 gas turbine jet engines, the sale of high performance computers, and licensed co-production of helicopters.

Nonetheless, the list of military-related technologies legally transferred to the PRC directly from the United States remains relatively small.

Illegal transfers of US technology from the US to the PRC, however, have been significant. Significant transfers of US military technology have also taken place in the mid-1990s through the re-export by Israel of advanced technology transferred to it by the United States, including

avionics and missile guidance useful for the PLA's F-10 fighter. Congress and several Executive agencies have also investigated allegations that Israel has provided US-origin cruise, air-to-air, and ground-to-air missile technology to the PRC.²⁶

Joint Ventures with US Companies

The vast majority of commercial business activity between the United States and the PRC does not present a threat to national security, but additional scrutiny, discipline, and an awareness of risks are necessary with respect to joint ventures with the PRC where the potential exists for the transfer of militarily-sensitive US technology.

The US 1997 National Science and Technology Strategy stated that: "Sales and contracts with foreign buyers imposing conditions leading to technology transfer, joint ventures with foreign partners involving technology sharing and next generation development, and foreign investments in US industry create technology transfer opportunities that may raise either economic or national security concerns."²⁷

The behavior of the PRC Government and PRC-controlled businesses in dealing with US companies involved with militarily sensitive technology confirms that these concerns are valid and growing. The growing number of joint ventures that call for technology transfers between the PRC and US firms can be expected to provide the PRC with continued access to dual-use technologies for military and commercial advantage.

Technology transfer requirements in joint ventures often take the form of side agreements (sometimes referred to as offset agreements) requiring both that the US firm transfer technology to the PRC partner, and that all transferred technology will eventually become the property of the PRC partner.²⁸

Although many countries require technology transfers when they do business with US firms, no country makes such demands across as wide a variety of industries as the PRC does.²⁹ Despite the

PRC's rapid economic liberalization since 1978, it continues to implement its explicitly designed goals and policies to restrict and manage foreign investment so as to bolster the PRC's military and commercial industries through acquisition of technology.³⁰

The Communist Party has long believed that forcing technology from foreign firms is not only critical to the PRC, but also is a cost that foreign firms will bear in order to obtain PRC market entry.

In the past, the PRC has favored joint ventures with US high-technology companies for several reasons:

- The US excels in many areas of technology that are of special interest to the PLA and to PRC-controlled firms
- Many PRC scientists were educated in the United States and retain valuable contacts in the US research and business community who can be exploited for technology transfer
- Many other countries are more reluctant than the United States to give up technology³¹

The PRC has dedicated increasing resources to identifying US high-technology firms as likely targets for joint venture overtures. Science and technology representatives in PRC embassies abroad are used to assist in this targeting of technology, and to encourage collaboration with US firms for this purpose.

Unless they are briefed by the FBI pursuant to its National Security Threat List program, US companies are unaware of the extent of the PRC's espionage directed against US technology, and thus—at least from the US national security standpoint—are generally unprepared for the reality of doing business in the PRC. They lack knowledge of the interconnection between the CCP, the PLA, the State, and the PRC-controlled companies with which they deal directly in the negotiating process.³²

The US General Accounting Office (GAO) has found that US businesses have significant concerns about arbitrary licensing requirements in the PRC that often call for increased technology transfer. The GAO has also found that transparency was the most frequent concern reported by US companies.³³ Because of the lack of transparency in the PRC's laws, rules, and regulations that govern business alliances, and the dearth of accessible, understandable sources of regulatory information, US businesses are often subjected to technology transfer requirements that are not in writing, or are not maintained in the field, or are contained in "secret" rules that only insiders know about.³⁴

The PRC's massive potential consumer market is the key factor behind the willingness of some US businesses to risk and tolerate technology transfers. Some of these transfers could impair US national security, as in the cases of Loral and Hughes. The obvious potential of the PRC market has increasingly enabled the PRC to place technology-transfer demands on its US trading partners.

US businesses believe that they must be in the PRC, lest a competitor get a foothold first.³⁵ In fact, many US high-technology firms believe it is more important to establish this foothold than to make profits immediately or gain any more than limited access to the PRC market.³⁶ Some of the PRC's trading partners have focused on increased technology transfers to raise the attractiveness of their bids.

In addition to traditional types of technology transfer, many US high-technology investments in the PRC include agreements establishing joint research and development centers or projects. This type of agreement represents a new trend in US investment in the PRC and is a potentially significant development.³⁷

US companies involved in joint ventures may be willing to transfer technology because they believe that the only risk is a business one - that is, that the transfers may eventually hurt them in terms of market share or competition.³⁸ These businesses may be unaware that technologies transferred to a

PRC partner will likely be shared within the PRC's industrial networks and with the PLA, or that joint ventures may be used in some instances as cover to acquire critical technology for the military.

COSTIND, which controls the PRC's military-industrial organizations, likely attempts to monitor technologies through joint ventures. In addition, US businesses may be unaware that joint-venture operations are also vulnerable to penetration by official PRC intelligence agencies, such as the MSS.

In one 1990s case reviewed by the Cox Committee, a US high-technology company and its PRC partner used a joint venture to avoid US export control laws and make a lucrative sale of controlled equipment to the PRC. Following the denial of an export license, the US company attempted to form a joint venture to which the technology would be transferred. The joint venture was controlled by a PRC entity included on the US Commerce Department's Entity List, which means it presents an unacceptable risk of diversion to the development of weapons of mass destruction.

Acquisition and Exploitation of Dual-Use Technologies

The acquisition of advanced dual-use technology represents yet another method by which the PRC obtains advanced technology for military modernization from the United States. The PRC's military modernization drive includes a policy to acquire dual-use technologies. The PRC seeks civil technology in part in the hope of being able to adapt the technology to military applications. Some analysts refer this to as "spinning on."³⁹

A strategy developed by the PRC in 1995 called for the acquisition of dual-use technologies with civil and military applications, and the transfer of R&D achievements in civil technology to the research and production of weapons.

The PRC collects military-related science and technology information from openly available

US and Western sources and military researchers. This accelerates the PLA's military technology development by permitting it to follow proven development options already undertaken by US and Western scientists.

PRC procurement agents have approached US firms to gain an understanding of the uses of available technology, and to evaluate the PRC's ability to purchase dual-use technology under the guise of civil programs and within the constraints of US export controls. Additionally, the PRC has attempted to acquire information from the US and other countries about the design and manufacturing of military helicopters.⁴⁰ The PRC could use this approach to acquire chemical and biological weapons technology.

The key organizations in the PRC's drive to acquire dual-use technology include:

- COSTIND acquires dual-use technology for PRC institutes and manufacturers by assuring foreign suppliers that the technology will be used for civil production. COSTIND uses overseas companies to target US firms for acquisition of dual-use technology for the military.
- The Ministry of Electronics Industry (MEI)⁴¹ is responsible for developing the PRC's military electronics industry. Among other things, the Ministry approves and prioritizes research and development and the importation of electronics technologies that can be used to speed up the PRC's indigenous production capabilities.
- The Ministry of Post and Telecommunications (MPT) is acquiring asynchronous transfer mode switches that could be used for military purposes by the PLA.⁴²
- PLA-operated import-export companies, which also import dual-use technologies for military modernization. Polytechnologies, a company attached to the General Staff Department of the PLA, plays a major role in this effort, especially in negotiating foreign weapons purchases.⁴³
- AVIC, and its subsidiary, China National Aero-Technology Import-Export Corporation (CATIC), which have sent visitors to US firms to discuss manufacturing agreements for commercial systems that could be used to produce military aircraft for the PLA. AVIC is one of five PRC state-owned conglomerates that operate as "commercial businesses" under the direct control of the State Council and COSTIND.

Several incidents highlight CATIC's direct role in the acquisition of controlled US technology. One clear example was CATIC's role as the lead PRC representative in the 1994 purchase of advanced machine tools from McDonnell Douglas.

Another possible example of the PRC's exploitation of civilian end-use as a means of obtaining controlled technology was CATIC's 1983 purchase of two US-origin CFM-56 jet engines on the pretext that they would be used to re-engine commercial aircraft. Although the CFM-56 is a commercial engine, its core section is the same as the core of the General Electric F-101 engine that is used in the US B-1 bomber. Because of this, restrictions were placed on the export license. However, the PRC may have exploited the technology of the CFM-56. When the US Government subsequently requested access to the engines, the PRC claimed they had been destroyed in a fire.

CATIC has, on several occasions, misrepresented the proposed uses of militarily useful US technology. The Clinton administration determined that the specific facts in these cases may not be publicly disclosed without affecting national security.

In 1996, AVIC, CATIC's parent company, attempted to use a Canadian intermediary to hire former Pratt & Whitney engineers in the United States to assist in the development of an indigenous PRC jet engine. AVIC's initial approach was under the guise of a civilian project, and the US engineers were not told they would be working on a military engine for the PRC's newest fighter jet until

negotiations had progressed substantially. The US engineers pulled out when they were told what they would be asked to do.⁴⁴

The degree of diversion to military programs by the PRC of commercially acquired technologies is unclear, since the PRC's parallel civil-military industrial complex⁴⁵ often blurs the true end-use of technology that is acquired. As a result, there may be more use of US dual-use technology for military production than these examples suggest.

Front Companies

Another method by which the PRC acquires technology is through the use of front companies. The term "front company" has been used in a variety of ways in public reports and academic studies in different contexts, and can include:

- US subsidiaries of PRC military-industrial corporations in the PRC
- US subsidiaries of PLA-owned-and-operated corporations
- Corporations set up by PRC nationals overseas to conduct technology acquisition and transfer
- Corporations set up outside the PRC to acquire technology for a PRC intelligence service, corporation, or institute covertly
- Corporations set up outside the PRC by a PRC intelligence service, corporation, or institute solely to give cover to professional or non-professional agents who enter the United States to gather technology or for other purposes
- Corporations set up outside the PRC by a PRC intelligence service to launder money
- Corporations set up outside the PRC by a PRC intelligence service to raise capital to fund intelligence operations

- Corporations set up outside the PRC by a PRC individual to hide, accumulate, or raise money for personal use.
- Corporations set up outside the PRC by organs of the PRC Government to funnel money to key US leaders for the purpose of garnering favor and influencing the US political process and US Government decision-making

The differing meanings attached to the term "front companies" by different US agencies has led to confusion, particularly because many PRC companies fall into several different categories, at the outset or at different times during their existence. In addition, US agencies responsible for different aspects of national security, law enforcement, and Sino-US relations often do not share even basic data concerning PRC espionage in the United States.

This may partly explain why, for example, in Senate testimony on the same day in 1997, the State Department said it could identify only two PLA companies that were doing business in the United States, while the AFL-CIO identified at least 12, and a Washington-based think-tank identified 20 to 30 such companies.⁴⁶ The Select Committee has determined that all three figures are far below the true figure.

The Select Committee has concluded that there are more than 3,000 PRC corporations in the United States, some with links to the PLA, a State intelligence service, or with technology targeting and acquisition roles. The PRC's blurring of "commercial" and "intelligence" operations presents challenges to US efforts to monitor technology transfers for national security purposes.

General Liu Huaqing, who recently retired as a member of the Communist Party Politburo, the CCP Standing Committee, and the Central Military Commission, was involved with dozens of companies in Hong Kong and in Western countries engaged in illegally acquiring advanced US technology.

Yet another complicating factor is the evolution of the names used by PRC-controlled corporations. Some corporations such as NORINCO and Polytechnologies were easily recognizable as subsidiaries of PRC corporations. The boards of directors of PRC companies were also easily recognizable as PLA officers in the past.⁴⁷ Recent changes, however, have made it more difficult to recognize PRC corporations.

Some analysts note that US-based subsidiaries of PLA-owned companies in particular have stopped naming themselves after their parent corporation, a move prompted at least in part by criminal indictments and negative media reports that have been generated in connection with their activities in the United States. Many PLA-owned companies in the United States have simply ceased to exist in the past year or so, a phenomenon that reflects these factors as well as the fact that PRC-controlled companies often do not make money.⁴⁸

The PRC intelligence services use front companies for espionage. These front companies may include branches of the large ministerial corporations in the PRC, as well as small one- and two-person establishments. Front companies, whatever the size, may have positions for PRC intelligence service officers. PRC front companies are often in money-making businesses that can provide cover for intelligence personnel in the United States.

PRC front companies may be used to sponsor visits to the US by delegations that include PRC intelligence operatives.

There has been increasing PRC espionage through front companies during the 1990s. As of the late 1990s, a significant number of front companies with ties to PRC intelligence services were in operation in the United States.

The PRC also uses its state-controlled “news” media organizations to gain political influence and gather political intelligence.

In June 1993, after a highly publicized trial, a former Chinese philosophy professor, Bin Wu,

and two other PRC nationals were convicted in a US court of smuggling third-generation night-vision equipment to the PRC. Wu worked at the direction of the MSS, which he says directed him to acquire numerous high-technology items from US companies. To accomplish these tasks, Wu and the others created several small front companies in Norfolk, Virginia. From that base, they solicited technology from a number of US companies, purchasing the equipment in the names of the front companies and forwarding it to the MSS through intermediaries in Hong Kong.⁴⁹

Wu was a good example of the non-traditional PRC approach to acquiring technology in that Wu himself was not a professional intelligence agent. Identified as a pro-Western dissident by the MSS just after the Tiananmen Square massacre, he was given a choice: he could stay in the PRC and face prison, or he could accept the MSS’s offer to help him and his family by supporting the PRC in its quest for high technology. Wu was also a “sleeper” agent, who was initially told to go to the United States and establish himself in the political and business community. The MSS told Wu he would be called upon and given taskings later.⁵⁰

Wu appears to have been part of a significant PRC intelligence structure in the United States. This structure includes “sleeper” agents, who can be used at any time but may not be tasked for a decade or more.⁵¹

In the 1990s, the PRC has also attempted to use front companies to acquire sensitive information on restricted military technologies, including the Aegis combat system. The Aegis combat system uses the AN/SPY-1 phased array radar to detect and track over 100 targets simultaneously, and a computer-based command and decision system allowing for simultaneous operations against air, surface, and submarine threats.⁵²

Direct Collection of Technology by Non-Intelligence Agencies and Individuals

PRC intelligence agencies often operate in the

US commercial environment through entities set up by other PRC Government and commercial organizations instead of creating their own fronts. PLA military intelligence officers do operate, however, directly in the United States, posing as military attaches at the PRC Embassy in Washington, D.C., and at the United Nations in New York.

Individuals attached to PRC Government and commercial organizations accomplish most PRC covert collection of restricted technology in the United States and are unaffiliated with official PRC intelligence services. These organizations collect their own technology from the United States, rather than rely on the PRC intelligence agencies to do it for them.

The Cox Committee judged that the MSS might be allowing other PRC Government entities to use MSS assets to fulfill their intelligence needs. These findings further illustrate that PRC “intelligence” operations are not necessarily conducted by what are traditionally thought of as “intelligence” agencies.

The main PLA intelligence activity in the United States is not represented by PLA intelligence organizations, but by PRC military industries and regular components of the PLA. Although military-industrial corporations are not PLA-owned, they are deeply involved in arms production and acquisition of military technology.

The activities of CATIC and its US subsidiaries exemplify the activities carried out by PRC military-industrial companies. Other PRC companies, such as China Great Wall Industry Corporation, collect technology for their own use and may be used as cover by PRC intelligence personnel.

Various science and technology commissions and organizations also carry out PRC technology acquisition in the United States. COSTIND, for example, has no official US subsidiary but is the primary coordinating authority over the military-industrial corporations that collect technology in

the United States. COSTIND also uses the “front company” device to procure high-technology products.

The PRC State Science and Technology Commission largely oversee civilian science and technology collection. The State Science and Technology Commission also use diplomats in the US as a key collection tool. It has provided funding to a PRC scientist to establish various commercial enterprises in the US as a means of collecting technology information for distribution in the PRC.

The State Science and Technology Commission was involved in efforts to elicit nuclear weapons information from a Chinese-American scientist. Science and Technology offices in the PRC’s seven diplomatic agencies in the United States carry out a substantial portion of technology acquisition taskings. The primary role of these offices is to arrange contacts between PRC scientists and their American counterparts.

Various “liaison groups” constitute another PRC technology collection vehicle in the United States. The PRC’s primary official liaison organization is the China Association for International Exchange of Personnel (CAIEP). CAIEP operates seven “liaison organization” offices in the United States, including one in Washington, D.C., and one in San Francisco. It is one of several organizations set up by the PRC to illegally acquire technology through contacts with Western scientists and engineers. Others include a purported technology company and a PRC State agency.

Another significant source of the PRC’s technology collection efforts outside of its formal intelligence agencies comes from Chinese business representatives loyal to the CCP who emigrate to the United States. These individuals pursue commercial interests independent of direct PRC Government control. Their primary motive is personal financial gain, and they will sell their efforts and opportunities to any willing consumer. When asked to do so, they pass US technology back to the PRC.

The PRC also acquires advanced technology through the outright theft of information. A few cases exemplify this method of technology acquisition of which the Peter Lee case represents a classic non-intelligence service operation.

Peter Lee is a naturalized US citizen who was born in Taiwan. Lee worked at Los Alamos National Laboratory from 1984 to 1991, and for TRW Inc., a contractor to Lawrence Livermore National Laboratory, from 1973 to 1984 and again from 1991 to 1997.

Lee has admitted to the FBI that, in 1997, he passed to PRC weapons scientists classified research into the detection of enemy submarines under water. This research, if successfully completed, could enable the PLA to threaten previously invulnerable US nuclear submarines.

Lee made the admissions in 1997 during six adversarial interviews with the FBI. According to Lee, the illegal transfer of this sensitive research occurred while he was employed by TRW, Inc., a contractor for the Lawrence Livermore National Laboratory. Lawrence Livermore developed the classified information as part of a joint US-United Kingdom Radar Ocean Imaging project for anti-submarine warfare applications.

In 1997, the decision was made to not prosecute Lee for passing this classified information on submarine detection to the PRC. Because of the sensitivity of this area of research, the Defense Department requested that this information not be used in a prosecution.

Throughout much of the 1990s, the FBI conducted a multi-year investigation of Peter Lee, employing a variety of techniques, but without success in collecting incriminating evidence. Finally, in 1997, Lee was charged with willfully providing to the PRC classified information on techniques for creating miniature nuclear fusion explosions.

Specifically, Lee explained to PRC weapons scientists how deuterium and tritium can be loaded into a spherical capsule called a target and

surrounded by a “hohlraum,” and then heated by means of laser bombardment. The heat causes the compression of these elements, creating a nuclear fusion micro-explosion. This so-called “inertial confinement” technique permits nuclear weapons scientists to study nuclear explosions in miniature—something of especial usefulness to the PRC, which has agreed to the ban on full-scale nuclear tests in the Comprehensive Test Ban Treaty.

Lee said that during a lecture in the PRC he answered questions and drew diagrams about hohlraum construction. In addition, Lee is believed to have provided the PRC with information about inertial confinement lasers that are used to replicate the coupling between the primary and secondary in a thermonuclear weapon.

Lee was formally charged with one count of “gathering, transmitting or losing defense information,” in violation of Section 793 of Title 18 of the US Code, and one count of providing false statements to a US government agency, in violation of Section 1001, Title 18. On December 8, 1997, Lee pled guilty to willfully passing classified US defense information to PRC scientists during his 1985 visit to the PRC. Lee also pled guilty to falsifying reports of contact with PRC nationals in 1997. Lee was sentenced to 12 months in a halfway house, a \$20,000 fine and 3,000 hours of community service.⁵³

The Cox Committee judged that, between 1985 and 1997, Lee might have provided the PRC with more classified thermonuclear weapons-related information than he has admitted. The PRC apparently co-opted Lee by appealing to his ego, his ethnicity, and his sense of self-importance as a scientist.

The Cox Committee also received evidence of PRC theft of technology data from US industry during the 1990s valued at millions of dollars. The PRC used Chinese nationals hired by US firms for that purpose. The Clinton administration has determined that no details of this evidence may be made public without affecting national security.

In 1993, PRC national Yen Men Kao, a North Carolina restaurant owner, was arrested by the FBI and charged with conspiring to steal and export classified and export-controlled high-technology items to the PRC.⁵⁴ Among the items about which Kao and several other PRC nationals were seeking information were:

- The US Navy's Mark 48 Advanced Capability Torpedo
- The F-404 jet engine used on the US F-18 Hornet fighter
- The fire-control radar for the US F-16 fighter⁵⁵

The case of Kao and his co-conspirators is one of several involving PRC commercial entities attempting to illegally acquire US technology.

The PRC also relies heavily on the use of professional scientific visits, delegations, and exchanges to gather sensitive technology.

As the PRC Government has increasingly participated in the world commercial and capital markets, the number of PRC representatives entering the United States has increased dramatically. One estimate is that in 1996 alone, more than 80,000 PRC nationals visited the United States as part of 23,000 delegations.

Almost every PRC citizen allowed to go to the United States as part of these delegations likely receives some type of collection requirement, according to official sources.

Scientific delegations from the PRC are a typical method used by the PRC to begin the process of finding US joint venture partners. These delegations have been known to go through the motions of establishing a joint venture to garner as much information as possible from the US partner, only to pull out at the last minute.

Scientific visits and exchanges by PRC scientists and engineers and their US counterparts create several risks to US national security. This has been a particular concern in recent years regarding

foreign visitors to the Department of Energy's national weapons laboratories.⁵⁶

The first of these risks is that visitors to US scientific and technology sites may exploit their initial, authorized access to information to gain access to protected information.⁵⁷ The Cox Committee reviewed evidence of PRC scientists who circumvented US restrictions on their access to sensitive manufacturing facilities.

Another risk is that US scientists may inadvertently reveal sensitive information during professional discussions.

The PRC subjects visiting scientists to a variety of techniques designed to elicit information from them. One technique may involve inviting scientists to make a presentation in an academic setting, where repeated and increasingly sensitive questions are asked.⁵⁸ Another is to provide the visitor with sightseeing opportunities while PRC intelligence agents burglarize the visitor's hotel room for information. Still another technique involves subjecting the visitor to a grueling itinerary and providing copious alcoholic beverages so as to wear the visitor down and lower resistance to questions.⁵⁹

In one instance, a US scientist traveled to the PRC where very specific technical questions were asked. The scientist, hesitant to answer one question directly because it called for the revelation of sensitive information, instead provided a metaphorical example. The scientist immediately realized that the PRC scientists grasped what was behind the example, and knew that too much had been said.

Another common PRC tactic is to tell US visitors about the PRC's plan for further research, the hope being that the US scientist will release information in commenting on the PRC's plans.

The Cox Committee reviewed evidence of this technique being applied to acquire information to assist the PRC in creating its next generation of nuclear weapons.

Another risk inherent in scientific exchanges is that US scientists who are overseas in the PRC are prime targets for approaches by professional and non-professional PRC organizations that would like to co-opt them into assisting the PRC. In many cases, they are able to identify scientists whose views might support the PRC, and whose knowledge would be of value to PRC programs.

The Cox Committee received information about Chinese-American scientists from US nuclear weapons design laboratories being identified in this manner. Typically, the PRC will invite such a scientist to lecture and, once in the PRC, question him closely about his work. Once the scientist has returned to the US, answers to follow-up questions may be delivered through a visiting intermediary. Such efforts to co-opt scientists may be conducted by PRC ministries, and may involve COSTIND.

The number of PRC nationals attending educational institutions in the United States presents another opportunity for the PRC to collect sensitive technology.⁶⁰ It is estimated that at any given time there are over 100,000 PRC nationals who either are attending US universities or have remained in the United States after graduating from a US university. These PRC nationals provide a ready target for PRC intelligence officers and PRC Government-controlled organizations, both while they are in the United States and when they return to the PRC.⁶¹

The Cox Committee judged that the PRC was increasingly looking to PRC scholars who remain in the United States as assets who have developed a network of personal contacts that can be helpful to the PRC's search for science and technology information.

The PRC has also acquired technological information through open forums such as arms exhibits and computer shows. During one international arms exhibit, for example, PRC nationals were observed collecting all possible forms of technical information. This included videotaping every static display and designating individuals to take notes. The group also stole a

videocassette from a display that was continuously playing information on the US Theater High Altitude Air Defense system, when the Defense Department contractor left it unattended. Converting the stolen cassette to a frame-by-frame sequence could yield valuable intelligence information to the PRC.⁶²

Illegal Export of Military Technology Purchased in the United States

The PRC is also taking advantage of the ongoing US military downsizing. In particular, PRC representatives and companies in the United States pursue the purchase of high-technology US military surplus goods.

In a single 1996-1997 operation, the Los Angeles office of the US Customs Service seized over \$36 million in excess military property that was being shipped overseas illegally. Among the seized US military surplus equipment on its way to the PRC and Hong Kong were:

- 37 inertial navigation systems for the US F-117 and FB-111 aircraft
- Thousands of computers and computer disks containing classified Top Secret and higher information
- Patriot missile parts
- 500 electron tubes used in the US F-14 fighter
- Tank and howitzer parts
- 26,000 encryption devices.⁶³

PRC representatives have been the biggest buyers of sensitive electronic surplus material. Defense Department investigators have noted a trend among the PRC buyers of this equipment: many had worked for high-technology companies in the PRC or for PRC Government science and technology organizations.⁶⁴

The PRC has been able to purchase these goods because, in its rush to dispose of excess property, the Defense Department failed to code properly or to disable large amounts of advanced military equipment, allowing PRC buyers to pay for and take immediate possession of functional high-

technology equipment. Often this equipment was purchased as “scrap,” for which the buyers paid pennies on the dollar.⁶⁵

According to the US Customs Service, many PRC companies that bid on military surplus technology intentionally used “American-sounding” names to mask their PRC affiliation.⁶⁶

The PRC also has been able to exploit US military downsizing by purchasing advanced technology, in the form of machine tools and production equipment from decommissioned US defense factories, through industrial auctions.

For example, a multi-axis machine tool profiler, designed to build wing spans for the US F-14 fighter, originally cost over \$3 million but was purchased by the PRC for under \$25,000.⁶⁷

According to one industrial auctioneer, the PRC frequents industrial auctions because they offer accurate, well-maintained equipment at bargain prices and with quick delivery.⁶⁸ Moreover, once the PRC obtains this equipment, there are ample resources available in the United States to upgrade the equipment to modern standards.

A California company specializing in refurbishing machine tools, for example, was approached in recent years by representatives of CATIC’s El Monte, California office. The CATIC representatives reportedly inquired about the scope of the company’s refurbishment capability, including whether it could train CATIC people to rebuild and maintain the machines and whether the company would be willing to assemble the machines in the PRC. The CATIC personnel also reportedly asked if the company could convert a three-axis machine tool to a five-axis machine tool. They were told this was possible for some machines, and very often only requires replacing one computer controller with another.⁶⁹

The US company noted, however, that such a converted machine would require an export license. In response, the CATIC personnel reportedly said, rather emphatically, that they would have

“no problem” with the export. The CATIC inquiries came at about the same time CATIC was negotiating the purchase of machine tools from the McDonnell Douglas Columbus, Ohio plant.

CATIC’s discussions with this particular US company did not result in either the training of CATIC personnel or the conversion of any machine tools. It is unknown, however, what other US companies were approached with similar inquiries or whether any such inquiries resulted in technological assistance to CATIC or the PRC.

The Cox Committee reviewed evidence from the mid-1990s of a PRC company that obtained US defense manufacturing technology for jet aircraft, knowingly failed to obtain a required export license, and misrepresented the contents of its shipping containers in order to get the technology out of the country. The Clinton administration determined that further information on this case could not be made public without affecting national security.

PRC Purchase of Interests in US Companies

A more recent method used by the PRC to obtain advanced technology from the United States is through the purchase of an interest in US high-technology companies or US export facilities. While this method does not yet appear to be prevalent, it has been identified in at least three instances.

In 1990, CATIC acquired an interest in MAMCO Manufacturing, a Seattle, Washington aircraft parts manufacturer. In a highly-publicized decision that year, President George Bush exercised his authority under section 721 of the Defense Production Act of 1950 (also known as the Exon-Florio provision) to order CATIC to divest itself of its MAMCO interest. This was based on the recommendations of the Committee on Foreign Investment in the United States (CFIUS), an inter-agency committee chaired by the Secretary of Treasury and tasked to conduct

reviews of foreign acquisitions that might threaten national security.⁷⁰

CFIUS concluded that:

- Some technology used by MAMCO, although not state-of-the-art, was export-controlled
- CATIC had close ties to the PLA through the PRC Ministry of Aviation (now known as AVIC)
- The acquisition would give CATIC unique access to US aerospace companies

It is likely that the PRC's strategy in acquiring MAMCO was to give CATIC a venue from which to solicit business with US aerospace firms, both to yield revenue and to gain access to aerospace technologies, inasmuch as CATIC has conspired to illegally acquire US sensitive technology in the past. In addition, according to public reports, CATIC has been used for PRC arms sales to countries such as Iran.

The PRC's efforts to acquire MAMCO did not end with President Bush's divestiture order. CATIC requested CFIUS approval to satisfy the concerns expressed in President Bush's divestiture order by selling its MAMCO interest to CITIC.

CFIUS noted that CITIC reported directly to the highest level of the PRC Government, the PRC State Council, and that CITIC did not have any colorable business rationale for wanting to acquire MAMCO. When CFIUS began questioning CITIC's business purposes and its ties to the State Council, CATIC withdrew its request.

CATIC then filed another request, this time proposing that it meet President Bush's divestiture order by selling its MAMCO interest to Huan-Yu Enterprises, a PRC company that was owned by a PRC provincial government and reported to the PRC MEI (now known as the Ministry of Information Industry), which in turn reported directly to the PRC State Council.

A CFIUS investigation concluded that Huan-Yu was a consumer, not a producer, of aerospace parts

and had no legitimate reason to acquire MAMCO. The proposed divestiture looked to CFIUS like a "sham acquisition." Faced with intense CFIUS interest, CATIC again withdrew its filing.

In 1996, Sunbase Asia, Incorporated purchased Southwest Products Corporation, a California producer of ball bearings for US military aircraft. Sunbase is incorporated in the United States, but is owned by an investment group comprised of some of the PRC's largest state-owned conglomerates as well as a Hong Kong company. According to a Southwest executive, the purchase will "take [Sunbase] to the next level" of technology.⁷¹ The Clinton administration determined that additional information on this transaction could not be made public without affecting national security.

China Ocean Shipping Company (COSCO), the PRC's state-owned shipping company which operates under the direction of the Ministry of Foreign Trade and Economic Cooperation and answers to the PRC State Council,⁷² attempted to lease port space that was being vacated by the US Navy in Long Beach, California. The lease proposal led to a heated debate between Congress, which wanted to prevent the lease based on national security concerns, and President Clinton, who supported the lease. Legislation passed by both houses of Congress in 1997 barred the lease and voided the President's authority to grant a waiver.⁷³

Other information indicates COSCO is far from benign. In 1996, US Customs agents confiscated over 2,000 assault rifles that were being smuggled into the United States aboard COSCO ships.⁷⁴ "Although presented as a commercial entity," according to the House Task Force on Terrorism and Unconventional Warfare, "COSCO is actually an arm of the Chinese military establishment." The Clinton administration determined that additional information concerning COSCO that appeared in the Cox Committee's classified Final Report could not be made public without affecting national security.

Methods Used by the PRC to Export Military Technology from the United States

Once the PRC acquires advanced technology in the United States, it requires secure means to export the information or hardware out of the country. Weaknesses in US customs can be exploited to smuggle classified or restricted US technology.

Diplomatic pouches and traveling PRC diplomats offer another avenue for illegal technology exports. Almost every PRC Government commercial and diplomatic institution in the United States has personnel who facilitate science and technology acquisitions.

The Cox Committee believed that these means of communicating with the PRC could have been exploited to smuggle nuclear weapons secrets from the United States.

These are some of the further means that have been used to illegally ship sensitive technology to the PRC:

- In 1993, Bin Wu, a PRC national, was convicted of transferring night-vision technology to the PRC. Wu used the US postal system to get technology back to the PRC. He mailed the technology he collected directly to the PRC, mostly through an intermediary in Hong Kong.⁷⁵
- The PRC uses false exportation documentation and has falsified end-user certificates. In one case reviewed by the Select Committee, the Department of Commerce reported that a US subsidiary of a PRC company used a common illegal export tactic when it falsely identified the machine tools it was exporting. The US Customs Service also indicated that the PRC's use of false bills of sale and false end-use statements are common illegal export tactics.
- The PRC has used at least one commercial air carrier to assist in its technology transfer efforts. In 1996, Hong Kong Customs officials intercepted air-to-air missile parts being shipped

by CATIC aboard a commercial air carrier, Dragonair. Dragonair is owned by CITIC, the most powerful and visible PRC-controlled conglomerate, and Civil Aviation Administration of China (CAAC).⁷⁶

- A common PRC method for transferring US technology to the PRC uses Hong Kong as the shipment point. This method takes advantage of the fact that US export controls on Hong Kong are significantly less restrictive than those applied to the rest of the PRC, allowing Hong Kong far easier access to militarily-sensitive technology.

The more relaxed controls on the export of militarily sensitive technology to Hong Kong have been allowed to remain in place even though Hong Kong was absorbed by the PRC and PLA garrisons took control of the region on July 1, 1997. US trade officials report that no inspections by the Hong Kong regional government or by any other government, including the United States, are permitted when PLA vehicles cross the Hong Kong border.

Various US Government analyses have raised concerns about the risk of the diversion of sensitive US technologies not only to the PRC, but to third countries as well through Hong Kong because of the PRC's known use of Hong Kong to obtain sensitive technology.⁷⁷ Some controlled dual-use technologies can be exported from the United States to Hong Kong license-free, even though they have military applications that the PRC would find attractive for its military modernization efforts.

The Cox Committee reported indications that a sizeable number of Hong Kong enterprises serve as cover for PRC intelligence services, including the MSS. Therefore, it is likely that over time, these could provide the PRC with a much greater capability to target US interests in Hong Kong.

US Customs officials also concur that transshipment through Hong Kong is a common PRC tactic for the illegal transfer of technology.⁷⁸

PRC Incentives for US Companies to Advocate Relaxation of Export Controls

US companies in the high-technology sector are eager to access the PRC market. The PRC often requires these US firms to transfer technologies to the PRC as a precondition to market access. US export regulations can be seen as an impediment to commercial opportunities.⁷⁹

Executives wishing to do business in the PRC share a mutual commercial interest with the PRC in minimizing export controls on dual-use and military-related commodities. The PRC has displayed a willingness to exploit this mutuality of interest in several notoriously public cases by inducing VIPs from large US companies to lobby on behalf of initiatives, such as export liberalization, on which they are aligned with the PRC.

The PRC is determined to reduce restrictions on the export of US communications satellites for launch in the PRC. From the perspective of the PRC, provision of such launch services creates a unique opportunity to consult with US satellite manufacturers, access information regarding US satellite technology, and obtain resources to modernize their rockets.⁸⁰ US satellite manufacturers are, in turn, anxious to access the potentially lucrative PRC market, and realize that launching in the PRC is a potential condition to market access.⁸¹

By agreeing to procure numerous satellites from Hughes Electronics Co. (Hughes) and Space Systems/Loral (Loral) in the early 1990s, the PRC created a mutuality of interest with two companies well-positioned to advocate the liberalization of export controls on these platforms.

For example, Bernard L. Schwartz, Chairman and CEO of Loral Space & Communications, Ltd., the parent company of Loral, met directly on at least four occasions with Secretary of Commerce Ron Brown after 1993, and accompanied him on a 1994 trade mission to the PRC.⁸²

C. Michael Armstrong, the former Chairman and Chief Executive Officer of GM Hughes Electronics, the parent company of Hughes, has served as Chairman of President Clinton's Export Council since 1993, working with the Secretary of State, the Secretary of Commerce, and others to "provide insight and counsel" to the President on a variety of trade matters.⁸³ Armstrong also served or had served as a member of the Defense Preparedness Advisory Council, the Telecommunications Advisory Council, and the Secretary of State's Advisory Council.⁸⁴

Both Armstrong and Schwartz, as well as other executives from high-technology firms, advocated the transfer of export licensing authority from the "more stringent control" of the State Department to the Commerce Department. Armstrong met with the Secretary of Defense, the National Security Advisor, and the Secretary of State on the matter, and both Schwartz and Armstrong co-signed a letter with Daniel Tellep of Lockheed-Martin Corporation to the President urging this change.⁸⁵ The changes they advocated were ultimately adopted.

Between 1993 and January 3, 1999, Loral and Hughes succeeded in obtaining waivers or export licenses for an aggregate of five satellite projects.⁸⁶

Another example of the incentive to advocate the relaxation of export controls involved the Charoen Pokphand Group (CP Group), Thailand's largest multinational company and one of the largest investors in the PRC. CP Group executives have served as economic advisors to the PRC Government and were chosen to sit on the committees dealing with the absorption of Hong Kong.⁸⁷

The CP Group was a founding member of Asia Pacific Telecommunications Satellite Holdings, Ltd. (APT), a consortium run by PRC-controlled investment companies, including China Aerospace Corporation. APT imports satellites manufactured by Hughes and Loral as part of the Apstar program for launch in the PRC by China Great Wall Industry Corporation.⁸⁸

On June 18, 1996, several CP Group executives attended a coffee with President Clinton at the White House. These executives included Dhanin Chearavanont (CP Chairman and Chief Executive Officer), Sumet Chearavanont (Vice Chairman and President), and Sarasin Virapol (employee and translator). The CP executives were invited to the coffee by their Washington, D.C., lobbyist, Pauline Kanchanalak.⁸⁹

According to one participant, Karl Jackson of the US-Thailand Business Council, the CP executives “dominated the conversation at the coffee.” The discussion included US-PRC relations, Most-Favored-Nation trade status for the PRC, and US technology. Other participants corroborate Jackson’s characterization of the role that CP executives played at the event.⁹⁰

PRC Theft of US Thermonuclear Warhead Design Information

The People’s Republic of China’s penetration of our national weapons laboratories spans at least the past several decades, and almost certainly continues today.

The PRC’s nuclear weapons intelligence collection efforts began after the end of the Cultural Revolution in 1976, when the PRC assessed its weaknesses in physics and the deteriorating status of its nuclear weapons programs.

The PRC’s warhead designs of the late 1970s were large, multi-megaton thermonuclear weapons that could only be carried on large ballistic missiles and aircraft. The PRC’s warheads were roughly equivalent to US warheads designed in the 1950s. The PRC may have decided as early as that time to pursue more advanced thermonuclear warheads for its new generation of ballistic missiles.

The PRC’s twenty-year intelligence collection effort against the US has been aimed at this goal. The PRC employs a “mosaic” approach that capitalizes on the collection of small bits of

information by a large number of individuals, which is then pieced together in the PRC. This information is obtained through espionage, rigorous review of US unclassified technical and academic publications, and extensive interaction with Department of Energy (DOE) laboratories and US scientists.

The Cox Committee judged that the PRC’s intelligence collection efforts to develop modern thermonuclear warheads were focused primarily on the Los Alamos, Lawrence Livermore, Sandia, and Oak Ridge National Laboratories.

As a result of these efforts, the PRC has stolen classified US thermonuclear design information that helped it fabricate and successfully test a new generation of strategic warheads.

The PRC stole classified information on every currently deployed US intercontinental ballistic missile (ICBM) and submarine-launched ballistic missile (SLBM). The warheads for which the PRC stole classified information include: the W-56 Minuteman II ICBM; the W-62 Minuteman III ICBM; the W-70 Lance short-range ballistic missile (SRBM); the W-76 Trident C-4 SLBM; the W-78 Minuteman III Mark 12A ICBM; the W-87 Peacekeeper ICBM; and the W-88 Trident D-5 SLBM. The W-88 warhead is the most sophisticated strategic nuclear warhead in the US arsenal. It is deployed on the Trident D-5 submarine-launched missile.

The PRC also stole classified information on US weapons design concepts, on weaponization features, and on warhead reentry vehicles (the hardened shell that protects a warhead during reentry).

The PRC may have acquired detailed documents and blueprints from the US national weapons laboratories.

The US Intelligence Community reported in 1996 that the PRC stole neutron bomb technology from a US national weapons laboratory. The PRC had previously stolen design information on the US W-70 warhead in the late 1970s; that earlier theft, which included design information, was discovered several months after it took place. The W-70 has elements that can be used as a strategic thermonuclear warhead or an enhanced radiation (“neutron bomb”) warhead. The PRC tested a neutron bomb in 1988.

The PRC may have also acquired classified US nuclear weapons computer codes from US national weapons laboratories. The Cox Committee believed that nuclear weapons computer codes remain a key target for PRC espionage. Nuclear weapons codes are important for understanding the workings of nuclear weapons and can assist in weapon design, maintenance, and adaptation. The PRC could make use of this information, for example, to adapt stolen US thermonuclear design information to meet the PRC’s particular needs and capabilities.

During the mid-1990s, it was learned that the PRC had acquired US technical information about insensitive high explosives. Insensitive high explosives are a component of certain thermonuclear weapons. Insensitive high explosives are less energetic than high explosives used in some other thermonuclear warheads, but have advantages for other purposes, such as thermonuclear warheads used on mobile missiles.

The PRC thefts from our national weapons laboratories began at least as early as the late 1970s, and significant secrets are known to have been stolen as recently as the mid-1990s. Such thefts almost certainly continue to the present.

How the PRC Acquired Thermonuclear Warhead Design Information from the United States: PRC Espionage and Other PRC Techniques

The Cox Committee judged that the PRC’s intelligence collection efforts to develop modern thermonuclear warheads focused primarily on the following US National Laboratories: Los Alamos, Lawrence Livermore, Oak Ridge, and Sandia. These efforts included espionage, rigorous review of US unclassified technical and academic publications, and extensive interaction with Department of Energy laboratories and US scientists.

Espionage played a central part in the PRC’s acquisition of classified US thermonuclear warhead design secrets. In several cases, the PRC identified lab employees, invited them to the PRC, and approached them for help, sometimes playing upon ethnic ties to recruit individuals.

The PRC also rigorously mined unclassified technical information and academic publications, including information from the National Technical Information Center and other sources. PRC scientists have even requested reports via e-mail from scientists at the US national weapons laboratories. Peter Lee, who had been a scientist at both Lawrence Livermore and Los Alamos National Laboratories and was convicted in 1997 of passing classified information to the PRC, gave the PRC unclassified technical reports upon request. The PRC also learned about conventional explosives for nuclear weapon detonation from reviewing unclassified technical reports published by Department of Energy national weapons laboratories.

PRC scientists have used their extensive laboratory-to-laboratory interactions with the United States to gain information from US scientists on common problems, solutions to nuclear weapons physics, and solutions to engineering problems. The PRC uses elicitation in these meetings, where it shows familiarity with US information in an effort to “prime the pump” in order to try to glean

information about US designs. US scientists have passed information to the PRC in this way that is of benefit to the PRC's nuclear weapons program.

The PRC's espionage operations, which use traditional intelligence gathering organizations as well as other entities, are aggressively focused on US weapons technology.

The PRC's Academy of Engineering Physics (CAEP), which is under COSTIND, is the entity in charge of the PRC's nuclear weapons program. It is responsible for the research and development, testing, and production of all of the PRC's nuclear weapons.

CAEP has pursued a very close relationship with US national weapons laboratories, sending scientists as well as senior management to Los Alamos and Lawrence Livermore. Members of CAEP's senior management have made at least two trips during the mid-to-late 1990s to US national weapons laboratories to acquire information and collect intelligence. These visits provided the opportunity for the PRC to collect intelligence. The presence of such PRC nationals at the US national weapons laboratories facilitated the PRC's targeting of US weapons scientists for the purpose of obtaining nuclear weapons information.

US and PRC lab-to-lab exchanges were ended in the late 1980s, but were resumed in 1993. Scientific exchanges continue in many areas including high-energy physics.⁹¹ Discussions at the US national weapons laboratories in connection with the foreign visitors program are supposed to be strictly limited to technical arms control and material accounting issues. Nonetheless, these visits and scientific conferences provide opportunities for the PRC to interact with US scientists outside of official meetings, and facilitate the PRC's targeting of US weapons scientists.

The US national weapons laboratories argue that there are reciprocal gains from the exchanges. DOE describes some of the insights gained from these exchanges as unique. On the other hand, PRC scientists have misled the US about their

objectives and technological developments. Despite considerable debate in Congress and the Executive branch, including several critical GAO reports, the US Government has never made a definitive assessment of the risks versus the benefits of scientific exchanges and foreign visitor programs involving the US national weapons laboratories.⁹²

How the US Government Learned of the PRC's Theft of Our Most Advanced Thermonuclear Warhead Design Information

The US Government did not become fully aware of the magnitude of the counterintelligence problems at DOE laboratories until 1995. The first indication of successful PRC espionage against the laboratories arose in the late 1970s. During the last several years, more information has become available concerning thefts of US thermonuclear warhead design information, and how the PRC may be exploiting it. A series of PRC nuclear tests conducted from 1992 to 1996 that furthered the PRC's development of advanced warheads led to suspicions in the US intelligence community that the PRC had stolen advanced US thermonuclear warhead design information.

The "Walk-In"

In 1995, a "walk-in" approached the CIA outside of the PRC and provided an official PRC document classified "Secret" that contained design information on the W-88 Trident D-5 warhead, the most modern in the US arsenal, as well as technical information concerning other thermonuclear warheads.

The CIA later determined that the "walk-in"⁹³ was directed by the PRC intelligence services. Nonetheless, the CIA and other Intelligence Community analysts that reviewed the document concluded that it contained US thermonuclear warhead design information. The "walk-in" document recognized that the US nuclear warheads

represented the state-of-the-art against which PRC thermonuclear warheads should be measured.

Over the following months, a multidisciplinary group from the US Government, including the DOE and scientists from the US national weapons laboratories, assessed the information in the document. DOE and FBI investigations focused on the loss of the US W-88 Trident D-5 design information, but they did not focus on the loss of technical information about the other five US thermonuclear warheads. A DOE investigation of the loss of technical information about the other five US thermonuclear warheads had not begun as of January 3, 1999, after the Cox Committee had completed its investigation. In addition, the FBI had not yet initiated an investigation as of January 3, 1999.

DOE reported that the PRC has in fact acquired some US computer codes, including: the MCNPT code; the DOT3.5 code; and the NJOYC code.⁹ MCNPT is a theoretical code that is useful in determining survivability of systems to electronic penetration and dose penetration in humans. DOT3.5 is a two-dimensional empirical code that performs the same kinds of calculations as MCNPT, except uses numerical integration. NJOYC acts as a numerical translator between DOT3.5 and MCNPT.

Given the limited number of nuclear tests that the PRC has conducted, the PRC likely needs additional empirical information about advanced thermonuclear weapon performance that it could obtain by stealing the US “legacy” computer codes, such as those that were used by the Los Alamos National Laboratory to design the W-88 Trident D-5 warhead. The PRC may also need information about dynamic three-dimensional data on warhead packaging, primary and secondary coupling, and the chemical interactions of materials inside the warhead over time.

The Cox Committee was concerned that no procedures were in place that would either prevent or detect the movement of classified information, including classified nuclear-weapons design

information or computer codes, to unclassified sections of the computer systems at US national weapons laboratories. The access granted to individuals from foreign countries, including students, to these unclassified areas of the US national weapons laboratories’ computer systems could make it possible for others acting as agents of foreign countries to access such information, making detection of the persons responsible for the theft even more difficult.

The Cox Committee believed that the PRC would continue to target its collection efforts not only on Los Alamos National Laboratory, but also on the other US National Laboratories involved with the US nuclear stockpile maintenance program. The PRC may also seek to improve its hydrostatic testing capabilities by learning more about the Dual-Axis Radiographic Hydrotest (DARHT) facility at Los Alamos.

US Government Investigations of Nuclear Weapons Design Information Losses

The Cox Committee received information about the US Government’s investigation of the PRC’s theft of classified US design information for the W-70 thermonuclear warhead. The W-70, which is an enhanced radiation nuclear warhead (or “neutron bomb”, also, has elements that can be used for a strategic thermonuclear warhead. In 1996, the US Intelligence Community reported that the PRC had successfully stolen classified US technology from a US Nuclear Weapons Laboratory about the neutron bomb.

This was not the first time the PRC had stolen classified US information about the neutron bomb. In the late 1970s, the PRC stole design information on the US W-70 warhead from Lawrence Livermore Laboratory. The US Government first learned of this theft several months after it took place. The PRC subsequently tested a neutron bomb in 1988.

The FBI developed a suspect in the earlier theft. The suspect worked at Lawrence Livermore National Laboratory, and had access to classified information including designs for a number of US thermonuclear weapons in the US stockpile at that time.

In addition to design information about the W-70, this suspect may have provided to the PRC additional classified information about other US weapons that could have significantly accelerated the PRC's nuclear weapons program.

Investigation of Theft of Design Information For the W-88 Trident D-5 Thermonuclear Warhead

The Cox Committee received information about the US Government's ongoing investigation of the loss of information about the W-88 Trident D-5 thermonuclear warhead design.

During the PRC's 1992 to 1996 series of advanced nuclear weapons tests, a debate began in the US Government about whether the PRC had acquired classified US thermonuclear weapons design information. DOE began to investigate. In 1995, following the CIA's receipt of evidence (provided by the PRC-directed "walk-in") that the PRC had acquired technical information on a number of US thermonuclear warheads, including not only the W-88 Trident D-5 but five other warheads as well, DOE's investigation intensified. That investigation, however, focused on the W-88 and not the other weapons.

Early in its investigation, DOE cross-referenced personnel who had worked on the design of the W-88 with those who had traveled to the PRC or interacted with PRC scientists. One individual who had hosted PRC visitors in the past emerged from this inquiry as a suspect by the spring of 1995. (Editor Note: *Although the Cox Committee did not refer to the suspect by name because of the ongoing investigation, Wen Ho Lee was later identified as the suspect.*)

Even after being identified as a suspect, the individual, who still had a security clearance, continued to work in one of the most sensitive divisions at Los Alamos National Laboratory, Division X, which handles thermonuclear weapons designs and computer codes. In this position, the suspect requested and received permission to hire a

PRC graduate student who was studying in the US for the summer.

In December 1998, the suspect traveled to Taiwan. Following his return from Taiwan in December 1998, he was removed from Division X.

The FBI initiated a full investigation in the middle of 1996. At the date of the Cox Committee's January 3, 1999 classified Final Report, the suspect continued to work at the Los Alamos National Laboratory, and continued to have access to classified information. (Editor Note: *See Wen Ho Lee and also Department of Energy, FBI, and Department of Justice Handling of the Espionage Investigation into the Compromise of Design Information on the W-88 Warhead elsewhere in the CI Reader.*)

Investigation of Additional Incidents

The Cox Committee reviewed one case that offers a troublesome example of the manner in which scientific exchanges in the PRC can be exploited for espionage purposes. The incident involved the inadvertent, bordering on negligent, disclosure of classified technical information by a US scientist lecturing in the PRC.

The US scientist, who was representing a US National Laboratory during a lab-to-lab exchange with a PRC laboratory, was pressured by PRC counterparts to provide a solution to a nuclear weapons-related problem. Rather than decline, the scientist, who was aware of the clear distinction between the classified and unclassified technical information that was under discussion, provided an analogy. The scientist immediately saw that the PRC scientists had grasped the hint that was provided and realized that too much had been said.

The PRC employs various approaches to co-opt US scientists to obtain classified information. These approaches include: appealing to common ethnic heritage; arranging visits to ancestral homes and relatives; paying for trips and travel in the PRC; flattering the guest's knowledge and intelligence;

holding elaborate banquets to honor guests; and doggedly peppering US scientists with technical questions by experts, sometimes after a banquet at which substantial amounts of alcohol have been consumed.

On average, the FBI has received about five security-related referrals each month from DOE. Not all of these concern the PRC. These referrals usually include possible security violations and the inadvertent disclosure of classified information. The FBI normally conducts investigations of foreign individuals working at the National Laboratories.

The Department of Energy's Counterintelligence Program at the US National Weapons Laboratories

With additional funds provided by Congress in 1998, DOE is attempting to reinvent its counterintelligence programs at the US national weapons laboratories to prevent continued loss of information to the PRC's intelligence collection activities.

Funding for DOE's counterintelligence program, including seven employees at DOE's headquarters, was \$7.6 million in Fiscal Year 1998. For Fiscal Year 1999, Congress has increased that amount to \$15.6 million. With the support of the Director of Central Intelligence and the Director of the FBI, the President issued Presidential Decision Directive 61 (PDD-61) in February 1998. PDD-61 requires that a senior FBI counterintelligence agent be placed in charge of DOE's program, which has been done.

PDD-61 also instructed that a counterintelligence report with recommendations be presented to the Secretary of Energy. The report was submitted to the Secretary on July 1, 1998, with 33 specific recommendations. The Secretary had 30 days to respond to the NSC. However, due to the transition from Secretary Pena to Secretary Richardson, the response was delayed. In late November 1998, the Secretary of Energy approved all substantive recommendations. In December 1998, the

Directors of the US National Laboratories agreed to the counterintelligence plan during a meeting with the Secretary of Energy. DOE is now implementing the plan.

The Secretary's action plan instructs the Directors of the US National Laboratories to implement the recommendations. It directs DOE's Office of Counterintelligence to fund counterintelligence positions at individual laboratories so that they work directly for DOE, not the contractors that administer the laboratories.

DOE was to create an audit trail to track unclassified computer use and protect classified computer networks. The action plan also directed the creation of counterintelligence training programs and a counterintelligence analysis program. (Editor's Note: *See The Redmond Report, which reviewed the counterintelligence program at the Labs.*)

The DOE was also implement stricter requirements for reporting all interactions with foreign individuals from sensitive countries, including correspondence by e-mail. Laboratory Directors would be responsible for scrutinizing foreign visitors, in coordination with DOE's Counterintelligence Office.

DOE would require counterintelligence polygraphs of those who work in special access programs (SAP) and sensitive areas with knowledge of nuclear weapons design, or actually have hands-on access to nuclear weapons (about 10 percent of the total cleared population within DOE. Such persons would also undergo financial reviews and more rigorous background investigations conducted through local field offices of the FBI.

The FBI reportedly has sent several agents to DOE in the last 10 years to try to improve the counterintelligence program, but has repeatedly been unsuccessful. A significant problem has been the lack of counterintelligence professionals, and a bureaucracy that "buried" them and left them without access to senior management or the Secretary of Energy. DOE's new

Counterintelligence Director now has direct access to the Secretary.

After traveling to the laboratories and interviewing counterintelligence officials, DOE's new Counterintelligence Director reported in November 1998:

The counterintelligence program at DOE does not even meet minimal standards ... there is not a counterintelligence [program], nor has there been one at DOE [the Department of Energy] for many, many years. DOE's counterintelligence program requires additional training, funding, and accountability, according to this counterintelligence official. At present, an Office of Personnel Management contractor conducts DOE's background investigations. The new Director's opinion is that the present background investigations are "totally inadequate" and "do [not] do us any good whatsoever."

Another problem area is that DOE's counterintelligence process presently does not have any mechanism for identifying or reviewing the thousands of foreign visitors and workers at the US national weapons laboratories. On one occasion reviewed by the Cox Committee, for example, scientists from a US National Laboratory met foreign counterparts in a Holiday Inn in Albuquerque, New Mexico, in order to circumvent their laboratory's security procedures.

One responsibility of DOE's new counterintelligence program would be to find out who visits the laboratories, including those from sensitive countries, what they work on while they visit, and whether their access is restricted to protect classified information. Mechanisms have been recommended to identify visitors and fully vet them. DOE will attempt to improve the database used for background checks.

Classified information has been placed on unclassified networks, with no system for either detection or reliable prevention. There are no intrusion detection devices to determine whether

hackers have attacked DOE's computer network. According to damage assessments reviewed by the Cox Committee, however, attacks on the computers at the US national weapons laboratories are a serious problem. E-mail is also a threat: the US national weapons laboratories cannot track who are communicating with whom. For example, over 250,000 unmonitored e-mails are sent out of the Sandia National Laboratory alone each week.

PRC Gains Sensitive Information from Hughes

Hughes attempted to launch two communications satellites from the PRC on Long March rockets, which exploded before reaching orbit, one in 1992 and one in 1995. Allegations regarding technology transfer arose in connection with failure analysis investigations conducted by Hughes employees in the aftermath of these failed launches. Specifically, in 1992 and 1995, China Great Wall Industry Corporation launched two Hughes satellites manufactured for Australian (Optus B2) and Asian (Apstar 2) customers from a PRC launch facility in Xichang, PRC.

Both satellites were launched on a Long March 2E rocket. In both cases, an explosion occurred after take-off and before separation of the satellite. Hughes investigated the causes of both of these failed launches and determined that the rocket was the cause of the failures.

In the course of the investigations, Hughes communicated technical information regarding the rocket to the PRC that assisted the PRC in improving the Long March 2E rocket. The activities of Hughes employees in connection with the investigation of the failed launch in 1992 resulted in the transmission to the PRC of technical information that appears to have been approved by a US Government representative but not properly licensed. In the case of the 1995 Hughes failure investigation, Hughes employees exported technical information that also was approved by a US Government representative but should not have been authorized for export to the PRC.

In both cases, Hughes disclosed information to the PRC that related to improving the Long March 2E fairing, a portion of the rocket that protects the payload during launch. Such information was outside the scope of the original licenses Hughes obtained from the State and Commerce Departments, respectively, with respect to the export and launch of the Optus B2 and Apstar 2 satellites. Hughes claims that the 1993 Optus B2 failure analysis disclosures were cleared in advance by US Government officials, but neither Hughes nor the pertinent US Government agencies retained records that would substantiate this claim fully.

The lessons learned by the PRC from Hughes during the 1995 Apstar 2 failure investigation are directly applicable to fairings on other rockets, including those used to launch PRC military satellites.

Although the Long March 2E has not been used since 1995, it is possible that the PRC may have transferred the lessons learned from this launch failure investigation to its ballistic missile programs. These lessons could lead to the development of a more reliable fairing for use with advanced payloads on military ballistic missiles.

Hughes obtained a clearance for the 1995 disclosures that was improperly issued by a Commerce Department official. Hughes was confident that the cause of the 1992 launch failure on the PRC's Long March 2E rocket was the fairing. Hughes then ascertained with more certainty that the fairing was responsible for the 1995 launch failure. Hughes required that the PRC take appropriate corrective measures so that future launches of Hughes satellites on the Long March 2E rocket could occur and be insured.

Hughes employees conveyed to the PRC the engineering and design information necessary to identify and remedy the structural deficiencies of the fairing. At the time of the 1992 failure, the export of both the satellite and any information that might improve the rocket were subject to State Department licensing jurisdiction.

Hughes knew that the fairing was part of the rocket and that a State Department license was required to discuss improvements with the PRC. Although Hughes did not have a license to disclose information to the PRC relating to improvement of the fairing, Hughes, nonetheless, made such disclosures. Hughes claims that the Defense Technology Security Administration monitor authorized each disclosure. Contemporaneous Hughes records partially support this assertion. The monitor says he doubts that he in fact approved the disclosure, but says he cannot fully recall these matters.

Neither Hughes nor any relevant U.S. Government agency has been able to produce records substantiating all of the claimed approvals. Even if such approvals were in fact given, they would have exceeded the authority of the Defense Technology Security Administration monitor since he was not empowered to expand the scope of the license granted by the State Department. The monitor also should have known that a separate license was needed for the launch failure analysis activities. By the time of the 1995 failure investigation, partial jurisdiction for commercial satellites had been transferred to the Commerce Department, but licensing for improvements to any part of the rocket, such as the fairing, remained with the State Department.

Hughes officials who were responsible for the launch failure investigation in 1995 knew that technical information that would improve the rocket, including the fairing, was still subject to State Department jurisdiction and was not licensed for export. Nonetheless, Hughes sought Commerce Department approval to disclose information regarding the fairing to the PRC. A Commerce Department official, without consulting with Defense Department or State Department experts, approved that disclosure, he says, on the assumption that the fairing was part of the satellite, not the rocket. He now acknowledges that this decision was a mistake.

The Defense Department recently determined that the information Hughes made available to the PRC was sufficiently specific to inform the PRC of the kinds

of rocket changes and operational changes that would make the Long March 2E, and perhaps other rockets, more reliable. In particular, Hughes assisted the PRC in correcting the deficiencies in its models of the stresses or loads (such as buffeting and wind shear) that the rocket and payload experience during flight.

There are differing views within the US Government as to the extent to which the information that Hughes imparted to the PRC may assist the PRC in its ballistic missile development. There is agreement that any such improvement would pertain to reliability and not to range or accuracy. It is not clear, at present, whether the PRC will use a fairing that was improved as a result of Hughes' disclosures in a current or future ballistic missile program. Currently-deployed PRC ballistic missiles do not use fairings, and the PRC's future mobile land-based intercontinental ballistic missiles will probably not use a fairing. However, fairings are used by the PRC in launching military communications satellites and could be used for a submarine-launched ballistic missile.

In the opinion of the Cox Committee's independent expert, Dr. Alexander Flax, fairing improvements could also be of benefit to multiple independently-targeted reentry vehicle (MIRV) development, should the PRC decide to move in that direction.

Hughes also provided the PRC with practical insight into diagnostic and failure analysis techniques for identifying and isolating the cause of a launch failure. Whether or not the structural improvements to the fairing suggested by Hughes are of immediate use to the PRC's missile programs, that information expanded the PRC's repertoire of available technical solutions to future problems that it may encounter in its space and missile programs.

Finally, the Cox Committee's independent expert has concluded that Hughes provided the PRC with the benefit of its engineering experience and expertise. As a result, PRC engineers better understand how to conduct a failure analysis and how to design and

build more reliable fairings for rockets: "This will stand them in good stead in developing fairings (or shrouds) for ballistic missiles."

LORAL Investigation of Intelsat Launch Failure Provides PRC with Sensitive Information

On February 15, 1996, a Long March 3B rocket carrying the US-built Intelsat 708 satellite crashed just after lift off from the PRC's Xichang launch center. This was the third launch failure in 38 months involving the PRC's Long March series of rockets carrying US-built satellite payloads. It also was the first commercial launch using the new Long March 3B. These events attracted intense attention from the international space launch insurance industry, and eventually led to a review of the PRC launch failure investigation by Western aerospace engineers.

The activities of the Western aerospace engineers who participated on the review team—The Independent Review Committee—sparked allegations of violations of US export control regulations. The review team was accused of performing an unlicensed defense service for the PRC that resulted in the improvement of the reliability of the PRC's military rockets and ballistic missiles.

The Intelsat 708 satellite was manufactured by Loral under contract to Intelsat, the world's largest commercial satellite communications services provider.

China Great Wall Industry Corporation, the PRC state-controlled missile, rocket, and launch provider, began an investigation into the launch failure. On February 27, 1996, China Great Wall Industry Corporation reported its determination that the Long March 3B launch failure was caused by a broken wire in the inner frame of the inertial measurement unit within the guidance system of the rocket. In March 1996, representatives of the space launch insurance industry insisted that

China Great Wall Industry Corporation arrange for an independent review of the PRC failure investigation.

In early April 1996, China Great Wall Industry Corporation invited Dr. Wah Lim, Loral's Senior Vice President and General Manager of Engineering and Manufacturing, to chair an Independent Review Committee that would review the PRC launch failure investigation. Lim then recruited experts to participate in the Independent Review Committee: four senior engineers from Loral, two from Hughes, one from Daimler-Benz Aerospace, and retired experts from Intelsat, British Aerospace, and General Dynamics.

The Independent Review Committee members and staff met with PRC engineers during meetings in Palo Alto, California, and in Beijing. During these meetings the PRC presented design details of the Long March 3B inertial measurement unit, and the committee reviewed the failure analysis performed by the PRC.

The Independent Review Committee took issue with the conclusions of the PRC investigation because the PRC failed to sufficiently explain the telemetry data obtained from the failed launch.

The Independent Review Committee members proceeded to generate a Preliminary Report, which was transmitted to China Great Wall Industry Corporation in May 1996 without prior review by any US Government authority. Before the Independent Review Committee's involvement, the PRC team had concluded that the most probable cause of the failure was the inner frame of the inertial measurement unit. The Independent Review Committee's draft report that was sent to the PRC pointed out that the failure could also be in two other places: the inertial measurement unit follow-up frame, or an open loop in the feedback path. The Independent Review Committee recommended that the PRC perform tests to prove or disprove all three scenarios.

After receiving the Independent Review Committee's report, the PRC engineers tested these

scenarios and, as a result, ruled out its original failure scenario. Instead, the PRC identified the follow-up frame as the source of the failure. The PRC final report identified the power amplifier in the follow-up frame to be the root cause of the failure.

According to the Department of Defense, the timeline and evidence suggests that the Independent Review Committee very likely led the PRC to discover the true failure of the Long March 3B guidance platform.

At the insistence of the State Department, both Loral and Hughes submitted "voluntary" disclosures documenting their involvement in the Independent Review Committee. In its disclosure, Loral stated that "Space Systems/Loral personnel were acting in good faith and that harm to US interests appears to have been minimal." Hughes' disclosure concluded that there was no unauthorized export as a result of the participation of Hughes employees in the Independent Review Committee.

Several US government offices, including the State Department, the Defense Technology Security Administration, the Defense Intelligence Agency, and other Defense Department agencies reviewed the materials, submitted by both Loral and Hughes in their disclosures to the State Department.

The Defense Department assessment concluded that "Loral and Hughes committed a serious export control violation by virtue of having performed a defense service without a license . . ."

The State Department referred the matter to the Department of Justice for possible criminal prosecution.

An interagency review team performed a review of the Independent Review Committee matter in 1998 to reconcile differences in the assessments of the other agencies. That interagency team concluded:

- The actual cause of the Long March 3B failure may have been discovered more quickly by

the PRC as a result of the Independent Review Committee report

- Advice given to the PRC by the Independent Review Committee could reinforce or add vigor to the PRC's design and test practices
- The Independent Review Committee's advice could improve the reliability of the PRC's rockets
- The technical issue of greatest concern was the exposure of the PRC to Western diagnostic processes, which could lead to improvements in reliability for all PRC missile and rocket programs

PRC Targeting of Advanced Machine Tools

The PRC is committed to the acquisition of Western machine tool technology, and the advanced computer controls that provide the foundation for an advanced aerospace industry. Although the PRC acquires machine tools from foreign sources in connection with commercial ventures, it also seeks foreign-made machine tools on a case-by-case basis to support its military armament programs.

Moreover, the proliferation of joint ventures and other commercial endeavors that involve the transfer or sale of machine tools to the PRC makes it more difficult for foreign governments and private industry to distinguish between civilian and military end-uses of the equipment.

CATIC's purchase of used machine tools from McDonnell Douglas, now part of Boeing, is one illustration of the complexities and uncertainties faced by private industry and the US Government in these endeavors.

Machine tools are essential to commercial industry, and high precision, multiple-axis machine tools broaden the range of design solutions for weapon components and structural assemblies. Parts and structures can be designed with advantages in weight and cost relative to what could be achieved

with less advanced machine tools. For military and aerospace applications, the level of manufacturing technology possessed by a country directly affects the level of military hardware that can be produced, and the cost and reliability of the hardware.⁹⁴

Case Study: McDonnell Douglas Machine Tools

The Cox Committee determined that the US Government was generally unaware of the extent to which the PRC has acquired machine tools for commercial applications and then diverted them to military end uses. The McDonnell Douglas case illustrates that the PRC will attempt diversions when it suits its interests.

At the request of Congress, the US GAO in March 1996 initiated a review of the facts and circumstances pertaining to the 1994 sale of McDonnell Douglas machine tools to CATIC. The GAO issued its report on November 19, 1996. The report can be summarized as follows:

- In 1992, McDonnell Douglas and CATIC agreed to co-produce 20 MD-82 and 20 MD-90 commercial aircraft in the PRC. Known as the Trunkliner Program, the aircraft were to serve the PRC's domestic "trunk" routes. In late 1994, a contract revision reduced the number of aircraft to be built in the PRC to 20, and added the purchase of 20 US-built aircraft.
- CATIC is the principal purchasing arm of the PRC's military as well as many commercial aviation entities. Four PRC factories, under the direction of AVIC and CATIC, were to be involved in the Trunkliner Program.
- In late 1993, CATIC agreed to purchase machine tools and other equipment from a McDonnell Douglas plant in Columbus, Ohio that was closing. The plant had produced parts for the C-17 transport, the B-1 bomber, and the Peacekeeper missile. CATIC also purchased four additional machine tools from McDonnell Douglas that were located at Monitor Aerospace

Corporation in Amityville, New York, a McDonnell Douglas subcontractor.

- The machine tools were purchased by CATIC for use at the CATIC Machining Center in Beijing—a PRC-owned facility that had yet to be built—and were to be wholly dedicated to the production of Trunkliner aircraft and related work. McDonnell Douglas informed the US Government that CATIC would begin construction of the machining center in October 1994, with production to commence in December 1995.
- In May 1994, McDonnell Douglas submitted license applications for exporting the machine tools to the PRC and asked that the Commerce Department approve the applications quickly so that it could export the machine tools to the PRC, where they could be stored at CATIC's expense until the machining facility was completed. Following a lengthy interagency review, the Commerce Department approved the license applications on September 14, 1994, with numerous conditions designed to mitigate the risk of diversion.
- During the review period, concerns were raised about the possible diversion of the equipment to support PRC military production, the reliability of the end user, and the capabilities of the equipment being exported. The Departments of Commerce, State, Energy, and Defense, and the Arms Control and Disarmament Agency, agreed on the final decision to approve these applications.
- Six of the machine tools were subsequently diverted to Nanchang Aircraft Company, a PRC facility engaged in military and civilian production over 800 miles south of Beijing. This diversion was contrary to key conditions in the licenses, which required the equipment to be used for the Trunkliner program and to be stored in one location until the CATIC Machining Center was built.

- Six weeks after the reported diversion, the Commerce Department suspended licenses for the four machine tools at Monitor Aerospace in New York that had not yet been shipped to the PRC. Commerce subsequently denied McDonnell Douglas's request to allow the diverted machine tools to remain in the unauthorized location for use in civilian production. The Commerce Department approved the transfer of the machine tools to Shanghai Aviation Industrial Corporation, a facility responsible for final assembly of Trunkliner aircraft. The diverted equipment was relocated to that facility before it could be misused.
- The Commerce Department did not formally investigate the export control violations until six months after they were first reported. The US Customs Service and the Commerce Department's Office of Export Enforcement are now conducting a criminal investigation under the direction of the Department of Justice.⁹⁵

PRC Targeting of US Jet Engines and Production Technology

The PRC's acquisition of aerospace and defense industrial machine tools from US and foreign sources has expanded its manufacturing capacity and enhanced the quality of military and civilian commodities that the PRC can produce.⁹⁶ These acquisitions will support the PRC's achievement of a key goal: the development of an aerospace industrial base that is capable of producing components and structural assemblies for modern manned aircraft and cruise missiles.⁹⁷

In the mid-1980s and early 1990s, the PRC apparently adopted a three-track approach to acquiring US equipment and technologies in order to advance its own military jet engine capabilities:

- The diversion of engines from commercial end uses
- Direct purchase
- Joint ventures for engine production

The PRC's acquisition targets suggest that it planned to acquire several families of jet engines that could be adapted to various military and commercial applications.⁹⁸

In 1983, the PRC legally acquired two General Electric (GE) CFM-56 jet engines, ostensibly to analyze the engines for a potential civil aircraft upgrade program. In the course of the export licensing process, the Defense Department insisted on restricting the PRC's use of the engines. Under the terms of the licensing agreement:

*No technical data was to be transferred with the engines; the Chinese were not to disassemble the engines; and finally, if the Trident [civil aircraft] retrofit program had not begun within 1 year of the engines' arrival, the engines were to be repurchased by the manufacturer. In addition, the Chinese offered to retrofit engines at a Shanghai commercial aircraft facility where GE personnel would be able to monitor Chinese progress.*⁹⁹

Defense Department officials were concerned because the CFM-56 hot sections are identical to those used in the engines that power the US F-16 and B-1B military aircraft.¹⁰⁰

The PRC later claimed that the CFM-56 engines were destroyed in a fire.¹⁰¹ More likely, however, is that the PRC violated the US end-use conditions by reverse engineering part of the CFM-56 to develop a variant for use in combat aircraft.¹⁰²

Despite the suspected reverse engineering of the two GE jet engines that were exported in 1983, GE reportedly signed a contract in March 1991 with the Shenyang Aero-Engine Corporation for the manufacture of parts for CFM-56 engines.¹⁰³ According to one source, Shenyang "put in place quality and advanced manufacturing systems to meet US airworthiness standards."¹⁰⁴

The PRC aggressively attempted to illegally acquire GE's F404 engine, which powers the US F-18 fighter.¹⁰⁵ The PRC likely intended to use the F404 jet engine in its F-8 fighter.¹⁰⁶ The PRC

succeeded in acquiring some F404 technology through an indirect route by purchasing the LM-2500, a commercial GE gas turbine containing the F404 hot section.¹⁰⁷

In addition, GE has reportedly proposed a joint venture with the PRC to manufacture the so-called CFM-56-Lite. The engine could power the PRC's planned AE-100 transport.¹⁰⁸

The PRC also has targeted large engines for aerospace and non-aerospace applications. The PRC's acquisition plans reportedly include Pratt & Whitney JT-8 series engines and technology to support its large aircraft projects, as well as marine derivatives of the GE LM-2500 for naval turbine propulsion projects.¹⁰⁹ Regarding the JT-8 series:

In August 1986, CATIC licensed the technology for the US Pratt and Whitney FT8 gas turbine engine, including joint development, production and international marketing rights. The FT8 is a development of the JT8D-219 aero-engine (used to power Boeing 727, Boeing 737, and MD-82 aircraft), and can produce 24,000 kW (33,000 hp). (It) represented another significant technical leap for China's gas turbine capability . . . Chinese students were also sponsored by Pratt and Whitney for graduate level aerospace training in the United States.¹¹⁰

The PRC's efforts to acquire compact jet engines can be traced to 1965, when the Beijing Institute of Aeronautics and Astronautics launched a project to copy the US Teledyne-Ryan CAE J69-T-41A.¹¹¹

The Teledyne engine powered the US Air Force AQM-34N Firebee reconnaissance drone, a number of which were shot down over the PRC during the Vietnam conflict.¹¹² The PRC's copy of the US turbojet, dubbed WP-11, began ground testing in 1971 and currently powers the PLA's HY-4 "Sadsack," a short-range anti-ship cruise missile.¹¹³

The PRC began work on cruise missile engines in the 1980s. The PRC's interest in developing long-range cruise missiles increased dramatically after

the 1991 Persian Gulf War, when the performance of US Tomahawk cruise missiles demonstrated the effectiveness of precision missile strikes using conventional warheads. However, technical challenges slowed Beijing's efforts. For this reason, the PRC has attempted to acquire foreign-built engines for technical exploitation. If the PRC succeeds in building cruise missile propulsion and guidance systems, then it would probably not have difficulty marketing cruise missiles to third world countries.¹¹⁴

In 1990, the PRC attempted to advance its cruise missile program by purchasing the Williams FJ44 civil jet engine.¹¹⁵ This compact turbofan was derived from the engine that powers the US Tomahawk cruise missile. The FJ44 engine might have been immensely valuable to the PRC for technical exploitation and even direct cruise missile applications.¹¹⁶ But the PRC's effort to acquire FJ44 engines was rebuffed.¹¹⁷

Case Study: Garrett Engines

The redundancy inherent in the PRC's three-track approach to advancing its military jet engine capabilities—diversion of engines from commercial use, direct purchase, and joint ventures—began to bear fruit in the early 1990s.¹¹⁸

The Cold War's end and a liberalization of Cold War-era export controls on dual-use products and technologies opened new opportunities for the PRC to acquire advanced jet engines and production capabilities. A notable opportunity developed in 1991 when, as part of an overall liberalization of export controls by the Coordinating Committee for Multilateral Export Controls (COCOM), the Commerce Department decontrolled a popular jet engine manufactured by Allied Signal's Garrett Engine Division.

Prior to 1991, the Garrett engine required an individual validated license that included restrictive conditions.

The Commerce Department's decision that Garrett jet engines were decontrolled ensured that they could be exported to the PRC without a license or US Government review. The decision also opened the way for a jet engine co-production arrangement sought by the PRC.

Negotiations for a co-production deal between Allied Signal and PRC officials progressed until July 1992, when the Defense Department learned of the plan.¹¹⁹ The Defense Department's reaction to the news sparked an interagency review of the Commerce Department's decision to decontrol the Garrett engines.

The co-production deal was terminated after the review demonstrated the potential national security implications of transferring jet engine production capabilities to the PRC.¹²⁰

PRC Targeting of Garrett Engines

The PRC's reported motivation for initiating the Garrett engine purchase was the PRC's requirement for a reliable, high-performance Western engine for its developmental K-8 military aircraft.¹²¹

PRC aerospace organizations involved in the project included:

- CATIC
- China Nanchang Aircraft Manufacturing Company
- China National South Aero-Engine and Machinery Company.¹²²

The PRC's access to the Garrett TFE-731 may have influenced its choice of small jet engines in general, and K-8 propulsion in particular. The PLA purchased a fleet of Learjets from the US on the understanding that the aircraft would be for civil use. It is suspected, however, that the PLA diverted both the aircraft and the engines for military purposes, including PLA reconnaissance missions.¹²³

US Government Approval of the Initial Garrett Engine Exports

In August 1989, Allied Signal applied for an export license to sell a variant of the TFE-731, the TFE-731-2A-2A, to the PRC. Four engines and spare parts were to be shipped.¹²⁴ The US Federal Aviation Administration (FAA) had certified the TFE-731-2A-2A as a “civil” engine.¹²⁵

According to Iain S. Baird, then-Deputy Assistant Secretary of Commerce for Export Administration, the Commerce Department had licensing authority for the civil engine regardless of its military (i.e., the PLA’s K-8 military aircraft) application.¹²⁶

The 1989 application for the export of the Garrett engines to the PRC raised concerns among officials at the Defense Technology Security Administration, which was the focal point for export policy guidance and license reviews within the Defense Department.¹²⁷

Given this Defense Department judgment, a condition was placed by the Commerce Department on the export license for the TFE-731-2A-2As:

*“There is to be no transfer of engine design or manufacturing technical data provided with this transaction.” [Emphasis added]*¹²⁸

COCOM also reviewed the case. Subsequently, the Commerce Department issued an Individual Validated License (number D032648) for the Garrett engines on May 30, 1990.¹²⁹

In December 1990, Allied Signal asked the Commerce Department for approval to sell an additional 15 of the TFE-731-2A-2A engines to the PRC.¹³⁰

These engines were reportedly to be used for the first production run of the PLA’s K-8 military aircraft, which were to be sold to Pakistan. The Defense Department and COCOM again reviewed the license application, and Defense requested conditions that would forbid the release of TFE-731-2A-2A “design methodology, hot section

repair/overhaul procedures and manufacturing information.”¹³¹

On June 12, 1991, the Commerce Department granted Individual Validated License D130990, which included the Defense Department’s recommended conditions.¹³²

Commerce Department Decontrol of the Garrett Jet Engines

In August 1991, Allied Signal requested that the FAA re-certify the TFE-731-2A-2A engine with a digital electronic engine controller.¹³³ The FAA had certified the engine in 1988 with an analog engine controller.¹³⁴

It is unclear from the available information whether the PRC requested this upgrade of the engine to include the digital electronic engine controller, or whether Allied Signal decided to upgrade the engine on its own initiative.¹³⁵

On September 1, 1991, the Commerce Department published revisions to the Export Administration Regulations to reflect liberalized export controls that had been agreed to by the United States and its COCOM partners.¹³⁶ The revised regulations decontrolled many jet engines, but continued to control exports of engines equipped with full authority digital engine control (FADEC) systems.¹³⁷

These militarily sensitive systems control jet engine operations to permit, among other things, maximum propulsion performance for manned and unmanned military air vehicles.¹³⁸

According to Defense Department records, Allied Signal sent a one-page document to the Commerce Department on September 30, 1991 representing that the TFE-731-2A-2A did not use a FADEC system, but instead used a less capable digital electronic engine controller (DEEC). For this reason, Allied Signal officials believed the TFE-731-2A-2A was completely decontrolled under the revised Export Administration Regulations and COCOM controls.¹³⁹

Technical experts at the Defense Technical Security Agency had already presented their analysis to Commerce Department officials, countering that the TFE-731-2A-2A contained a FADEC and therefore remained controlled under COCOM and US regulations.¹⁴⁰

On October 1, 1991, one day after receiving the Allied Signal document regarding the FADEC issue, the Commerce Department ruled that the TFE-731-2A-2A did not contain a FADEC. The Commerce Department then informed Allied Signal's Garrett Engine Division that it could export TFE-731-2A-2A jet engines to the PRC under a General License (a so-called G-DEST license) pursuant to the Export Administration Regulations, as long as production technology was not transferred.¹⁴¹

Defense Department records indicate that officials at the Defense Technology Security Administration concurred with the Commerce Department decision to permit this export, but mistakenly believed it was still under an Individual Validated License arrangement - that is, with the requested Defense Department conditions.¹⁴²

Subsequently, the Commerce Department amended the October 1, 1991 decision and notified Allied Signal on November 25, 1991 that it had decontrolled the TFE-731-2A-2A entirely.¹⁴³

Engine production technology could now be exported to the PRC without a license.¹⁴⁴ According to Defense Department records, Commerce Department officials relied exclusively on Allied Signal's September 30, 1991 representation concerning the engine controller for the TFE-731-2A-2A - that is, that the controller was not a FADEC, and thus was no longer controlled.¹⁴⁵

Bruce C. Webb, then a senior analyst at the Commerce Department's Office of Nuclear Controls, recalls that a US Government advisory group had reviewed the Allied Signal document and agreed with the company's assertion that the TFE-731-2A-2A was not equipped with an embargoed

FADEC.¹⁴⁶ However, in response to document requests by the Select Committee, the Commerce Department was unable to provide any records of any technical reviews that it may have conducted.¹⁴⁷

The Interagency Review of the Proposed Export of Garrett Engines

Iain Baird, then-Deputy Assistant Secretary of Commerce for Export Administration, claims that the Commerce Department coordinated with appropriate agencies before making the General License determination in November 1991. However, the Commerce Department was unable to provide the Select Committee with any documentary evidence to this effect.¹⁴⁸

A Defense Technology Security Administration staff member suggests that other agencies learned of the decision by chance, or "dumb luck." In addition, according to a December 29, 1992 Defense Department memorandum for the record:

Commerce approved, with DoD and COCOM concurrence, the sale of 15 Garrett TFE-731-2A-2A engines to the PRC for incorporation into military trainers being exported to Pakistan.

In July 1992 DTSA [the Defense Technology Security Administration] learned from cable traffic that the PRC and Garrett were negotiating an arrangement to co-produce this engine in China for use in PLA military trainers.

We learned shortly thereafter that Department of Commerce had determined in November 1991 that the engine did not require an Individual Validated License (IVL) for shipment to the PRC.

Department of Commerce, without consulting with Department of Defense, classified the engine and technology decontrolled (or "G-DEST") under the COCOM Core List implemented on 1 September 1991.

DTSA believes the export requires an IVL [Individual Validated License].¹⁴⁹

After receiving a copy of the July 1992 cable, the Defense Technology Security Administration initiated an interagency review of the Commerce Department General License decision regarding the Garrett engines.¹⁵⁰ The Commerce Department agreed to suspend its decision pending the outcome of the review.

Officials at the Defense Technology Security Administration reportedly were especially concerned over any transfer of jet engine production technology to the PRC. They were also surprised that the Commerce Department opted not to coordinate its decision, given the agency's oft-repeated concerns over any transfer of jet engine production technology to the PRC.¹⁵¹

The Commerce Department's decision to decontrol Garrett engine technology was considered in the context of several US policies. Two policies in particular dominated the interagency debate: the 1991 Enhanced Proliferation Control Initiative (EPCI), and COCOM controls on jet engine technologies.

Consideration of Enhanced Proliferation Control Initiative Regulations

The Enhanced Proliferation Control Initiative was established by the Bush administration to provide a non-proliferation "safety net." It was intended to restrict the export of technologies usable for chemical and biological weapons or missiles, regardless of whether such technologies were controlled under existing international agreements (for example, under the 1987 Missile Technology Control Regime).

As explained by the Commerce Department:

Foreign policy controls are being imposed on certain exports by adopting a policy of denial for items that already require a validated license, for any reason other than short supply, where the export is determined to be for a facility involved in the development, production, stockpiling, delivery, or use of chemical or biological weapons or of missiles.

The purpose of these controls is to prevent American contribution to, and thereby distance the United States from, the proliferation of chemical and biological weapons and missile development.

These controls serve to demonstrate US opposition to the spread of these weapons and provide specific regulatory authority to control exports from the United States of commodities or technology where there is a significant risk that they will be used for these purposes. [Emphasis added]¹⁵²

According to the August 1991 interim Enhanced Proliferation Control Initiative regulations, the Commerce Department should have conducted a "case-by-case" review of Allied Signal's proposed export to determine whether it "would make a material contribution to the proliferation of missiles." If the export were "deemed to make such a contribution, the license [would] be denied."¹⁵³

Baird states that an Enhanced Proliferation Control Initiative review was not conducted for the engines, but was conducted for the production technology: "As far as the engines went, sending the whole engine up, we didn't feel it raised EPCI concerns. As far as the technology went, we did." Baird did not further explain the basis for the Commerce Department decision that the Garrett engines themselves did not require an Enhanced Proliferation Control Initiative review; nor did he explain why the technology did raise EPCI concerns.¹⁵⁴

The Department of Commerce was unable to provide the Select Committee with any records of the Enhanced Proliferation Control Initiative review it conducted for the Garrett engine production technology.¹⁵⁵

Allied Signal's partners in the Garrett engine transaction included:

- CATIC
- China Nanchang Aircraft Manufacturing Company

-
- The China National South Aero-Engine and Machinery Company

A 1992 US Government review of these proposed end users found that the export of Garrett engine production technology to the PRC could pose a national security threat to the United States.

The review found that PRC co-production of Garrett TFE-731-2 engines would enable Beijing to develop higher quality turbojet and turbofan engines for use in military and civilian aircraft and in cruise missiles. PRC access to this production process would also give Beijing the means to extend the range of its cruise missiles. This was of special concern because PLA missiles, rockets, and aircraft are produced at facilities also used for civilian production.

A Garrett representative confirmed that the Zhuzhou South Motive Power and Machinery Complex was the intended producer of the Garrett TFE-731-2 engine. There was concern that a flow-through of applicable production technologies to the PRC's cruise missile engine program was almost inevitable.¹⁵⁶

A copy of a US turbojet engine reportedly now powers the PLA's HY-4 cruise missile.¹⁵⁷ In addition, the conditions placed on the export of the Garrett engine technology of course would not prevent the PRC from reverse engineering the engine if that were the PRC's intent.¹⁵⁸

Each of the PRC participants in the Garrett engine co-production venture produces military hardware. Despite the assurances of Allied Signal that the engines it proposed to produce in the PRC would be used entirely for commercial purposes, PLA personnel were prominent in the negotiations with Garrett. The CATIC representatives were the same individuals who were prominent in the Committee on Foreign Investment in the United States (CFIUS) case involving the attempted purchase of MAMCO, a Boeing contractor, by CATIC. This is the only CFIUS case in which the President reversed a sale on national security grounds.¹⁵⁹

Because the PRC could incorporate complete TFE-731-2A-2A engines or modified variants directly into cruise missile airframes, export to the PRC of the engines themselves - as well as the production technology - presented a national security threat.¹⁶⁰

Consideration of COCOM and Export Administration Regulations

COCOM and Export Administration Regulation reviews were conducted to assess sensitive components in the Garrett TFE-731-2A-2A jet engine.

When Allied Signal's Garrett Engine Division upgraded the TFE-731-2A-2A with the addition of a digital engine controller, it claimed that the new system did not require an export license under the revised Export Administration Regulations and COCOM controls. It was determined that COCOM had not developed an agreed-upon technical definition to distinguish restricted from unrestricted engine controllers.¹⁶¹ This shortfall in the regime set the stage for an extended interagency debate over the status of the TFE-731-2A-2A vis-à-vis COCOM regulations.

The Defense Department believed the Garrett engines contained an embargoed, full authority digital engine control (FADEC) system. Moreover, the Defense Department obtained new information about improvements to the Garrett TFE-731-2A-2A that raised additional national security concerns.¹⁶²

Regarding the FADEC issue, the Defense Department acquired analysis and technical studies from numerous sources. A Defense Technology Security Administration analysis explained, for example:

The Garrett engine contains what [Allied Signal] calls a Digital Electronic Engine Control (DEEC) but describes in company literature as "full-authority, automatic engine control." DTSA maintains that the DEEC is a FADEC for the following reasons:

*FAA certification officials state in writing that the “DEEC” controller is a FADEC. Also DoD experts at the Air Force Aeronautical Systems Center and the Naval Air Warfare Center have assessed that the Garrett engine controller is a FADEC.*¹⁶³

Additional confirmation of these findings was contained in a technical paper developed by the engineering staff at the Defense Technology Security Administration:

In summary, the entire DoD Category 9 [aero-engines] negotiating team to COCOM during 1990-91 . . . are in agreement after detailed analysis, with assistance from experts in controls from Navy, Air Force and FAA, of data proprietary to Allied-Signal and otherwise, that the ASCA [Allied Signal Controls & Accessories division] DEEC, P/N 2118002-202 is a FADEC.

Allied-Signal’s memo to DTSA . . . shows this is indeed the FADEC utilized on the GED [Garrett Engine Division] TFE731-2A-2A engine.

The Defense Department inquiry found further that Allied Signal initially did not provide accurate information to the FAA during the civil certification process for the TFE-731-2A-2A:

FAA engineers rebuked GED [Garrett] in 1988 for their claim that the -2A engine was a direct derivation from a -2 engine rather than being derived from a TFE731-3. GED subsequently provided FAA with a corrected derivation showing that the engine was actually a TFE731-3 with TFE-731-3B parts and components rather than TFE731-2 components.

Substantial improvement to the TFE731-2A engine occurred when the so-called “Extended Life Turbine Modifications” were added during December, 1991, only one month after DOC [Commerce] had notified GED it had decontrolled the engine.

The Extended Life Turbine (ELT) resulted from the NASA program to obtain significant reductions in noise and emission levels, i.e., decreased infrared (IR) signature. The ELT has an enhanced damage tolerance and changes TFE731-series engines from an expected life of approximately 6,000 hours to 10,000 hours.

In summary, the engine GED [Garrett] submitted for a ‘paper certification’ as a TFE731-2A in 1988 was not a derivative of a -2 engine but was derived from a TFE731-3 with a TFE731-3B LP compressor. The changes noted above were included in the 1988 engine, i.e., the A5 seal and both LP compressor and turbine blades changed. The ELT was added in 1991.

In conjunction with the slight derating of the engine in 1988, life expectancy of this engine is greatly enhanced over a TFE731-3 turbofan engine; it is more durable, reliable, and generally more appropriate for use on military aircraft.

No applications of this engine to civil airframes are known to have been attempted by Allied-Signal, only military.¹⁶⁴ [Emphasis added]

The evidence obtained by the Defense Department indicated that the TFE-731-2A-2A was not simply a 20-year old engine for business jets, as Allied Signal and Commerce Department officials had claimed.¹⁶⁵ (Indeed, as of January 3, 1999, the TFE-731-2A-2A has never been used in a business jet.)¹⁶⁶

It is true that the engine had been derived from the TFE-731-3, an engine used in both civil and military applications, including the Cessna Citation III business jet and the CASA C-101BB ground-attack jet. But the engine had been upgraded with a new turbine to lower its infrared signature, thus improving the combat survivability of the aircraft in which it would be contained - for example, through the ability to escape detection by surface-to-air missiles.¹⁶⁷

Resolution of the Garrett Engine Controversy

The Garrett engine controversy was ultimately resolved through an interagency agreement at the Deputy Assistant Secretary level. Regarding the disputed engine controller, the Deputy Assistant Secretary of Defense for Counterproliferation Policy, Mitchel B. Wallerstein, described an interagency compromise in a March 21, 1994 letter to the Deputy Assistant Secretary for Export Controls at the State Department:

Defense is prepared to agree with the Allied (and Commerce) determination that the engine does not include a Full Authority Digital Engine Control System (FADEC) which meets the IVL [Individual Validated License] criteria. With respect to the 2A-2A engine, our proposed carve out from the definition of FADEC would provide a basis for a Commerce G-DEST classification, which would allow sales of the 2A-2A engine to the PRC, including its military, without prior [US Government] review and approval. It is unclear whether such a definitional carve out would require multilateral coordination with our current allies before such a G-DEST classification is made.¹⁶⁸

The State Department agreed with this proposal, and stated further: “We do not believe that it is necessary to coordinate multilaterally with our COCOM partners before moving to G-DEST treatment.”¹⁶⁹

Peter M. Leitner, senior trade advisor at the Defense Technology Security Administration, believes that the “definitional carve out” entailed a political decision to change the definition of the engine controller in order to circumvent export regulations and, in this case, avoid a COCOM review. According to Leitner, “you come up with some unique definition of the item and try to exempt or carve out coverage of that item in the regulations.”¹⁷⁰

Baird believes that COCOM reviewed the export license application for the upgraded variant of the Garrett TFE-731-2A-2A.¹⁷¹ Webb believes

COCOM did not review the application.¹⁷² The Commerce Department was unable to provide records of any COCOM review conducted for the upgraded Garrett engines.¹⁷³

Defense Department records indicate that some US government officials believed a COCOM review of the upgraded engines was essential. Without such a review, the United States might be seen by its partners as attempting to “circumvent CoCom controls.”¹⁷⁴

Wallerstein interprets the reference to “a carve out from the definition of FADEC” to mean that the disputed FADEC engine controller would be removed or modified to ensure that the TFE-731-2A-2A could be exported without controlled technology.¹⁷⁵ However, Wallerstein does not recall seeing any technical proposal from Allied Signal to modify the engine controller.¹⁷⁶

The documentary record suggests that the final, upgraded variant of the Garrett TFE-731-2A-2A was never submitted for a review by COCOM, which ceased operations in April 1994.¹⁷⁷

The status of the Garrett engines vis-à-vis the Enhanced Proliferation Control Initiative was largely resolved on August 19, 1993 during a meeting of the Commerce Department-chaired Operating Committee on Export Policy. According to a record of the meeting:

*Commerce, State and Defense have agreed to treat these commodities as if they were controlled. Moreover, [Allied Signal] has agreed not to transfer any co-production technology relating to these engines to the PRC.*¹⁷⁸

This interagency decision was finalized and reported in the news media in October 1995. As the Wall Street Journal reported then:

Allied Signal already has shipped about 40 built-up engines to China under the liberalized post-Cold War export rules, and isn't being deterred from exporting 18 more that the Chinese have ordered.

But when it sounded out the US Commerce Department last summer about its coproduction plan, the company was told that if it formally applied for a license to do so the application would be denied under the rules of the Enhanced Proliferation Control Initiative. The company decided not to apply for the license.¹⁷⁹

Between 1992 and 1996, Allied Signal reportedly exported 59 of these TFE-731-2A-2A jet engines to the PRC. Beijing's main interest was in acquiring a production capability for the engines; thus, it halted further orders when co-production plans were scuttled.¹⁸⁰

The PRC Continues to Acquire Jet Engine Production Processes

The PRC is continuing its effort to acquire production processes for US jet engines. For example, Pratt & Whitney Canada, a subsidiary of Connecticut-based United Technologies, in February 1996 became "the first foreign company to establish an aviation parts manufacturing joint venture in China (with Chengdu Engine Company)."¹⁸¹ The Chengdu Engine Company manufactures components for, among other purposes, large jet engines used in Boeing aircraft.¹⁸² The Chengdu factory also manufactures parts for the PRC's WP13 turbojet engine, which powers the PLA's F-8 fighter.¹⁸³ In 1997, a new joint venture was reportedly proposed for Chengdu.

A consortium of Pratt and Whitney, Northrop Grumman and Hispano-Suiza are offering a new aero-engine, the PW6000, specifically designed to power the AE-100 transport, and are planning to establish an aero-engine joint venture at Chengdu, Sichuan Province.¹⁸⁴

United Technologies operates additional aviation joint ventures with Xi'an Airfoil Technology Company and China National South Aero-Engine and Machinery Company. These ventures are largely comprised of manufacturing jet engine "cold section" components or producing relatively low-technology "hot section" components.¹⁸⁵

Endnotes

¹ Testimony of Nicholas Eftimiades, October 15, 1998.

² Interview of James Lilley, November 17, 1998.

³ Deng Xiaoping died 19 February 1997.

⁴ For the official report on this program, see "Decade-Long Hi-Tech Program Bears Fruit," Xinhua News Agency, September 27, 1996.

⁵ Su Kuoshan, "Road of Hope-Reviewing the Accomplishment of the '863' Project on the 10th Anniversary of its Implementation," Jiefangjun Bao, April 5, 1996, reproduced in Foreign Broadcast Information Service, Daily Report, May 8, 1996, FBIS-CHI-96-089.

⁶ Major Mark Stokes, "China's Strategic Modernization: Implications for US National Security," USAF Institute for National Security Studies, July 1998.

⁷ Cui Ning, "Hi-Tech Projects Highlight Five Areas," China Daily, April 3, 1996; in FBIS. See also Ding Henngao, COSTIND Director, speech delivered on March 28, 1996, "Review of the 863 Plan over the Past Ten Years"; Stokes.

⁸ These individuals often jump many bureaucratic levels to take their positions. Tai Ming Cheung, See, e.g., "China's Princelings," Kim Eng Securities, January 1995; Murray Scot Tanner and Michael Feder, "Family Politics, Elite Recruitment, and Succession in Post-Mao China," Australian Journal of Chinese Affairs, July 1993.

⁹ Interview of James Mulvenon, October 16, 1998.

¹⁰ See Murray Scot Tanner and Michael Feder, "Family Politics, Elite Recruitment, and Succession in Post-Mao China," Australian Journal of Chinese Affairs, July 1993.

¹¹ James Mulvenon, "Chinese Military Commerce and US National Security," RAND, July 1997; David Jackson, "US Probes Whether Beijing Gave Money to Influence Policy," Chicago Tribune, February 14, 1997.

¹² Ibid.

¹³ Tracy Connor, "New Asiagate Figure Has Military History," New York Post, November 7, 1998.

¹⁴ Interim Report of the House Government Reform and Oversight Committee ("HGROC Report") Chapter IV C.

¹⁵ Deposition of Shen Jun before the Select Committee (Dec. 8, 1998); Japanese Firms Buy Into Satellite Telephone Co., Information Access Newsbytes (July 9, 1996).

¹⁶ See generally, "Liu's Deals with Chung: An Intercontinental Puzzle," David Jackson and Lena H. Sun, *Washington Post*, May 24, 1998.

¹⁷ Interim Report of the House Government Reform and Oversight Committee ("HGROC Report") Chapter IV C.

¹⁸ Ibid.

¹⁹ Ibid.

²⁰ Ibid.

²¹ “Red Face Over China; Did a Chinese plot persuade Clinton to let a US company give China its rocket science? No. Politics (and policy) did,” Eric Pooley et. al., *Time*, June 1, 1998.

²² Interim Report of the House Government Reform and Oversight Committee (“HGROC Report”) Chapter IV C. “Liu’s Deals with Chung: An Intercontinental Puzzle,” David Jackson and Lena H. Sun, *Washington Post*, May 24, 1998.

²³ Testimony of James Mulvenon, RAND, before the Select Committee (Oct. 15, 1998); John Frankenstein and Bates Gill, “Current and Future Challenges Facing Chinese Defense Industries,” *China Quarterly* (June 1996).

²⁴ Bates Gill and Taeho Kim, “China’s Arms Acquisitions from Abroad, A Quest for Superb and Secret Weapons,” Stockholm International Peace Institute, Oxford University Press, 1995.

²⁵ *Ibid.*

²⁶ Shawn L. Twing, “Congress Calls for Sanctions if Israeli Technology Transfer to China is Proven,” *The Washington Report*, November/December 1996. See also Bates Gill and Taeho Kim, “China’s Arms Acquisitions from Abroad, A Quest for Superb and Secret Weapons,” Stockholm International Peace Institute, Oxford University Press, 1995; Tony Capaccio, “Israeli Arms Transfers of US Technology Remain and Abrasive Issue,” *Defense Week*, June 5, 1995.

²⁷ “The National Security Science and Technology Strategy,” US Office of Science and Technology Policy, 1996.

²⁸ Kathleen Walsh, “US Technology Transfers to the People’s Republic of China,” DFI International, December, 1997.

²⁹ Paul Blustein, “China Plays Rough: Invest and Transfer Technology, or No Market Access,” *Washington Post*, October 25, 1997.

³⁰ Kathleen Walsh, December, 1997.

³¹ Walsh, December, 1997, (stating the United States is “somewhere in the middle” among countries in its willingness to transfer technology).

³² Testimony of Nicholas Eftimiades, October 15, 1998.

³³ See “Challenges and Opportunities for US Businesses in China,” testimony of JayEtta Hecker, GAO, before the Committee on Banking and Financial Services, US House of Representatives, July 29, 1996.

³⁴ Interview of John Foorde, September 23, 1998.

³⁵ See, e.g., Walsh, December, 1997; Letter to the Select Committee from Sandra Taylor, Vice-President, Eastman Kodak Company, November 18, 1998.

³⁶ Walsh, December 1997. See also Joseph Kahn, “McDonnell’s Hopes in China Never Got Off the Ground,” *The Wall Street Journal*, May 22, 1996 (quoting McDonnell’s President as saying it should do “whatever it takes” to “carve out a place” in China).

³⁷ Walsh Testimony and Letter to the Select Committee from Sandra Taylor, Vice-President, Eastman Kodak Company, November 18, 1998.

³⁸ Letter to the Select Committee from Sandra Taylor, Vice-President, Eastman Kodak Company, November 18, 1998.

³⁹ See John Frankenstein, “China’s Defense Industries: A New Course?” The Chinese concept of a “spin-on” is in marked contrast to the “spin-off” approach of the US at the end of the Cold War, where the goal was to convert military technology to commercial uses.

⁴⁰ “News Digest,” *Helicopter News*, March 28, 1997. “The Z-11 is a reverse-engineered copy of Eurocopter’s single-engined Ecureuil.”

⁴¹ This Ministry is now known as the Ministry of Information Industry.

⁴² “Sale of Telecommunications Equipment to China,” Karen Zuckerstein, David Trimble, and John Neumann, General Accounting Office, November 1996.

⁴³ Testimony of James Mulvenon, October 15, 1998.

⁴⁴ Interview of Tom Nangle, October 8, 1998.

⁴⁵ Almost all Chinese military production lines are co-located with civil/commercial production lines.

⁴⁶ “Commercial Activities of China’s People’s Liberation Army (PLA),” Hearing Before the Committee on Foreign Relations, United States Senate, November 6, 1997.

⁴⁷ Testimony of James Mulvenon, October 15, 1998.

⁴⁸ *Ibid.*

⁴⁹ Interview of Bin Wu, October 20, 1998. See also John Fialka, “War by Other Means,” W.W. Norton and Co., New York (1997).

⁵⁰ *Ibid.*

⁵¹ *Ibid.*

⁵² “Aegis Combat System,” United States Navy Fact File.

⁵³ Letter from FBI Director Louis Freeh to Chairman Christopher Cox and Ranking Member Norman Dicks, November 10, 1998. Peter Lee refused to cooperate with the Cox Committee’s investigation on the advice of his lawyer not to testify before, or provide information to, the Cox Committee.

⁵⁴ Ronald Ostrow, “FBI Arrests Chinese National in Spy Ring Investigation,” *Los Angeles Times*, December 5, 1993; Bill Gertz, “Spy Sting Gets Chinese Man Deported,” *The Washington Times*, December 22, 1993.

⁵⁵ Ibid.

⁵⁶ "DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," Gary L. Jones et. al., General Accounting Office, September 1997.

⁵⁷ Ibid.

⁵⁸ "Chinese Spies Just as Active as Soviets Ever Were, FBI Says," Ruth Sinai, Associated Press, March 9, 1992. Statements in article are attributed to Patrick Watson, the FBI's Deputy Assistant Director for Intelligence.

⁵⁹ Testimony of Nicholas Eftimiades, October 15, 1998.

⁶⁰ "Chinese Intelligence Operations," Nicholas Eftimiades, Naval Institute Press, 1994.

⁶¹ Ibid.

⁶² "Chinese spy openly at weapons fair," Kenneth R. Timmerman, *The Washington Times*, March 24, 1997.

⁶³ "Department of Defense Disposition of Government Surplus Items," hearing before the Senate Judiciary Subcommittee on Administrative Oversight and the Courts, July 8, 1997; "Defense Inventory: Action Needed to Avoid Inappropriate Sales of Surplus Parts," General Accounting Office, August, 1998; "On the Introduction of The Arms Surplus Reform Act of 1997," statement by Rep. Pete Stark in the US House of Representatives, October 1, 1997.

⁶⁴ Ibid.

⁶⁵ Ibid.

⁶⁶ US Customs briefing to Select Committee Staff, October 28, 1998. In response to this situation, in October 1997, Representative Pete Stark introduced H.R. 2602, the Arms Surplus Reform Act of 1997, to place a moratorium on all surplus arms sales until DOD certified to Congress that steps had been taken to correct weaknesses in the surplus sales program. The Act did not pass, but a section was added to the Defense authorization Act for Fiscal Year 1998, Pub. L. 105-85, Sec. 1067, requiring similar steps. The DOD submitted its report to Congress in June, 1998, identifying problem areas and steps taken to address them.

⁶⁷ Robert Greenberger, "Let's Make a Deal: Chinese Find Bargains in Defense Equipment as Firms Unload Assets," *Wall Street Journal*, October 21, 1998; Dr. Stephen Bryen and Michael Ledeen, "China-Related Challenges," *Heterodoxy*, April/May 1997 (Submission for the record by Rep. Tillie Fowler in the US House of Representatives, June 26, 1997).

⁶⁸ Robert Levy, President, Norman Levy Associates, as quoted in Robert Greenberger, "Let's Make a Deal: Chinese Find Bargains in Defense Equipment as Firms Unload Assets," *Wall Street Journal*, October 21, 1998.

⁶⁹ Interview of Jerry Remick, October 8, 1998; Interview of David Duquette, October 14, 1998. In a response to

written interrogatories, officials of CATIC, USA denied it was aware of the existence of the US company. Letter to Daniel Silver from Barbara Van Gelder, October 22, 1998.

⁷⁰ "Message to the Congress on the China National Aero-Technology Import and Export Corporation Divestiture of MAMCO Manufacturing, Incorporated," The White House, February 1, 1990.

⁷¹ Bruce Einhorn, "The China Connection," *Business Week*, August 5, 1996: "Sunbase Asia Acquires Specialty Bearing Company," PR Newswire, January 17, 1996.

⁷² Briefing by US Treasury Department to Select Committee staff, October 29, 1998.

⁷³ See, e.g., Stan Crock, "China and the US: The Sparks May Start Flying," *Business Week*, November 16, 1998; Robert Little, "Controversial Carrier," *The Baltimore Sun*, November 8, 1998.

⁷⁴ See, e.g., Timothy Maier, "Long March Reaches Long Beach," *Insight*, September 8, 1997.

⁷⁵ Interview of Wu Bin, October 20, 1998.

⁷⁶ Bruce Smith, "Dragonair Misstep," *Aviation Week and Space Technology*, September 16, 1996; "Michael Mecham, "China Expands Stake in Cathay, Dragonair," *Aviation Week and Space Technology*, May 6, 1996.

⁷⁷ See, e.g., "Hong Kong's Reversion to China: Effective Monitoring Critical to Assess US Nonproliferation Risks," GAO, May, 1997.

⁷⁸ US Customs briefing to Select Committee Staff, October 28, 1998.

⁷⁹ Kathleen A. Walsh, "US Technology Transfers to the People's Republic of China," 1997.

⁸⁰ Testimony of Loren Thompson, Clayton Mowry and Ray Williamson, November 13, 1998; deposition of C. Michael Armstrong, November 17, 1998.

⁸¹ Deposition of Bernard L. Schwartz, November 21, 1998; testimony of Clayton Mowry, November 13, 1998.

⁸² Deposition of Bernard L. Schwartz, November 21, 1998.

⁸³ Deposition of C. Michael Armstrong, December 17, 1998.

⁸⁴ Ibid.

⁸⁵ Deposition of C. Michael Armstrong, December 17, 1998; letter from C. Michael Armstrong, Bernard L. Schwartz, and Daniel Tellep to the President, October 6, 1995.

⁸⁶ Aerospace Industries Association, "Presidential Satellite Waivers and Other Related Launch Information" (http://www.aia-aerospace.org/homepage/china_table1), October 26, 1998.

⁸⁷ Far Eastern Economic Review, January 23, 1997.

⁸⁸ Deposition of Bansang Lee, November 16, 1998. CP divested itself of its holdings in APT in late 1997. See Jonathan Sprague and Julian Gearing Bangkok, "Past Ambitions Catch Up To Charoen Pokphand," Asiaweek, May 15, 1998.

⁸⁹ SCGA Report.

⁹⁰ Testimony of Karl Jackson before the SCGA, September 16, 1997; testimony of Clark Southall Wallace before the SCGA, September 16, 1997; testimony of Beth Dozoretz before the SCGA, September 16, 1997.

⁹¹ Premier Zhu Rongji recently praised the efforts and progress of PRC and US scientists who attended the 19th Meeting of the Sino-US Joint Committee on High Energy Physics. Reportedly, Zhu expressed pleasure that the "two nations have conducted wide-ranging in-depth exchanges during the meeting and put forward many helpful proposals, which will not only be conducive to the development of high energy physics in PRC and the US, but also help expand scientific and technological cooperation between the two countries." An area of concern is the PRC intelligence practice of mining even ostensibly cooperative scientific exchanges for useful information. "Premier Meets US Science Group," China Daily, November 18, 1998.

⁹² See Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories, Government Accounting Office, October 1988; DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories, Government Accounting Office, September 1997; and, DOE Needs to Improve Controls Over Foreign Visitors To Its Weapons Laboratories, Government Accounting Office, October 14, 1998.

⁹³ A "walk-in" is an individual who voluntarily offers to conduct espionage. The Encyclopedia of Espionage defines a "walk-in" as "an unheralded defector or a dangle, a 'walk-in' is a potential agent or a mole who literally walks into an embassy or intelligence agency without prior contact or recruitment." See the Spy Book: The Encyclopedia of Espionage, by Norman Polmar and Thomas B. Allen (RH Reference & Information Publishing, Random House). The individual who approached the CIA in 1995 is suspected of being a "directed walk-in": a "walk-in" purposefully directed by the PRC to provide this information to the United States. There is speculation as to the PRC's motives for advertising to the United States the state of its nuclear weapons development.

⁹⁴ Department of Defense, The Militarily Critical Technologies List. Part I: Weapons Systems

Technologies (Washington, D.C.: US Department of Defense, June 1996).

⁹⁵ The machine tool diversion reportedly remains under investigation by the Department of Justice.

⁹⁶ DIA report, 1995. See also The Militarily Critical Technologies List. Part I: Weapons Systems Technologies, Department of Defense, June 1996, sec. 10; and "Report of Foreign Travel," Ronald V. Miskell, US Department of Energy, February 1998.

⁹⁷ China Today: Defense Science and Technology, Xie Guang, ed., Beijing National Defense Industry Press, 1993; and Gearing up for High-Tech Warfare, Richard Bitzinger and Bates Gill, Center for Strategic and Budgetary Assessments, 1996. ⁸⁰ See also The Militarily Critical Technologies List. Part I: Weapons Systems Technologies, Department of Defense, June 1996, sec. 1.

⁹⁸ "PLAAF & Aviation Production Overview," Kenneth W. Allen, Henry L. Stimson Center, Washington, D.C., 1998.

⁹⁹ Background Paper, Defense Intelligence Agency, 1993.

¹⁰⁰ Ibid.

¹⁰¹ Memorandum for the Record, December 17, 1998. William Schneider described this incident during a briefing on the dual-use applications of high performance computers. William Schneider, briefing on "High Performance (HPC) Exports to China," October 1, 1998. See also Defense Intelligence Agency, 1993.

¹⁰² Defense Intelligence Agency, 1993.

¹⁰³ Background Paper, Defense Intelligence Agency, 1993.

¹⁰⁴ Export Controls: Change in Export Licensing Jurisdiction for Two Sensitive Dual-Use Items GAO/NSIAD-97-24, January 1997, p. 5, (B22); and The Militarily Critical Technologies List. Part I: Weapons Systems Technologies, Department of Defense, June 1996, sec. 1.

¹⁰⁵ Memorandum for the Record, October 30, 1998.

¹⁰⁶ "PLAAF & Aviation Production Overview," Kenneth W. Allen, Henry L. Stimson Center, Washington, D.C., 1998.

¹⁰⁷ China's Aerospace Industry, Jane's Information Group, 1997, pp. 67, 70, (B172); and "PRC Gas Turbine Acquisition Efforts" Memorandum by Peter Leitner, Defense Technology Security Administration, September 1, 1992.

¹⁰⁸ China's Aerospace Industry, Jane's Information Group, 1997.

¹⁰⁹ Ibid.

¹¹⁰ "PRC Gas Turbine Acquisition Efforts" Memorandum by Peter Leitner, Defense Technology Security

Administration, September 1, 1992; and “Garrett Engine Case,” Memorandum from Peter Leitner, DTSA, to Barbara Dixon, Defense Intelligence Agency, July 21, 1992.

¹¹¹ China’s Aerospace Industry, Jane’s Information Group, 1997.

¹¹² “WP-11 Engine Information,” James Clauson, Jane’s Information Group, June 26, 1996.

¹¹³ Ibid.

¹¹⁴ Memorandum for the Assistant Secretary of Defense for International Security Affairs, January 7, 1993.

¹¹⁵ “Cruise Control: Relaxed US Export Controls Could Help China Build Stealthier and Longer-Range Cruise Missiles, Pentagon Officials Claim,” Nigel Holloway, Far Eastern Economic Review, August 14, 1997; and “Williams FJ44,” Jane’s All the World’s Aircraft 1990-1991, Jane’s Information Group, 1990.

¹¹⁶ “Morphing the Silkworm,” Dennis Gormley and Gregory DeSantis, Pacific-Sierra Research Corporation, Arlington, Virginia, Presentation to the Rumsfeld Commission, June 3, 1998; and China’s Aerospace Industry, Jane’s Information Group, 1997.

¹¹⁷ “Cruise Control: Relaxed US Export Controls Could Help China Build Stealthier and Longer-Range Cruise Missiles, Pentagon Officials Claim,” Nigel Holloway, Far Eastern Economic Review, August 14, 1997.

¹¹⁸ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹¹⁹ Memorandum for the Record, Review of State Department Cables Regarding Allied Signal/Garrett Jet engine Negotiations with the PRC, December 17, 1998. The relevant State Department cable- DTG 161312Z July 92, #0148838-0148839-was sent to Commerce, State and Defense. See also “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹²⁰ A history of the Garrett case is presented in “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of

Defense (Trade Security Policy) and DTSA Director, December 21, 1992. See also “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC,” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992.

¹²¹ “NAMC/PAC K-8 Karakorum,” Richard L. Aboulafia, World Military & Civil Aircraft Briefing, Teal Group Corp., Arlington, Virginia, March 1998.

¹²² “NAMC/PAC K-8 Karakorum,” Richard L. Aboulafia, World Military & Civil Aircraft Briefing, Teal Group Corp., Arlington, Virginia, March 1998.

¹²³ Memorandum from Peter Leitner to Peter Sullivan, Defense Technology Security Administration, December 30, 1992.

¹²⁴ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹²⁵ “Type Certification Data Sheet No. E6WE,” Federal Aviation Administration, March 23, 1998.

¹²⁶ The Federal Aviation Administration can certify a jet engine as “civil” if it meets certain safety and other requirements for civil aviation. Military engines that meet such requirements can be certified as civil through this process. A civil certification places the engines on the Commerce Control List, giving Commerce authority to license exports, pursuant to Export Administration Act Section 17(c) on Civil Aircraft Equipment. However, Section 17(c) states that Commerce has jurisdiction over civil aircraft equipment that “is to be exported to a country other than a controlled country.” The PRC was a “controlled country” during the time of the Garrett case. Iain Baird believed that in-as-much as the statute mandated inclusion of civil aircraft engines to some destinations on the Commerce Control List (CCL), it was decided to put the item as a whole on the list. Commerce was unable to provide a formal legal analysis of 17 (c) with respect to exports of civil aircraft equipment to controlled countries. Civil certification issues and EAA Section 17(c) are discussed in, Interview of Iain S. Baird, November 17, 1998; and Interview of Bruce C. Webb, December 2, 1998. For the response to the Select Committee’s request for records regarding commodity jurisdiction, see letter from John F.

Sopko, Chief Counsel for Special Matters, Department of Commerce, to Chairman Christopher Cox and Ranking Member Norm Dicks, December 14, 1998.

¹²⁷ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹²⁸ Ibid.

¹²⁹ Ibid.

¹³⁰ Ibid.

¹³¹ Ibid.

¹³² Ibid.

¹³³ Ibid.

¹³⁴ “Type Certification Data Sheet No. E6WE,” Federal Aviation Administration, March 23, 1988.

¹³⁵ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹³⁶ Ibid.

¹³⁷ The revised Export Administration Regulations are presented in Export Administration Regulations, Department of Commerce, Bureau of Export Administration, 1991, sections 9A01 and 9E03. FADECs are described in Interview of Bruce C. Webb, December 2, 1998; and The Militarily Critical Technologies List. Part I: Weapons Systems Technologies, Department of Defense, June 1996, sec.1.

¹³⁸ Interview of Bruce C. Webb, December 2, 1998.

¹³⁹ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁴⁰ Ibid.

¹⁴¹ Ibid.

¹⁴² Ibid.

¹⁴³ Commerce Form Letter to Allied Signal from Commerce Licensing Officer E.G. Christiansen, Subject: Advice on Amendment Request Returned Without Action, November 25, 1991; “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVLD130990,” Memorandum

from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁴⁴ “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC,” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992.

¹⁴⁵ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁴⁶ Interview of Bruce C. Webb, December 2, 1998.

¹⁴⁷ For the request for records, see letter from Chairman Christopher Cox and Ranking Member Norm Dicks to William M. Daley, Secretary of Commerce, November 20, 1998. For Commerce’s response, see letter from John F. Sopko, Chief Counsel for Special Matters, Department of Commerce, to Chairman Christopher Cox and Ranking Member Norm Dicks, December 14, 1998.

¹⁴⁸ For the request for records, see letter from Chairman Christopher Cox and Ranking Member Norm Dicks to William M. Daley, Secretary of Commerce, November 20, 1998. ¹³⁹ Interview of Peter Leitner, November 24, 1998.

¹⁴⁹ “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC,” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992.

¹⁵⁰ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁵¹ “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992; and “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum

from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁵² “Report to the Congress: Imposition of Foreign Policy Export Controls Under the Enhanced Proliferation Control Initiative,” Department of Commerce, Bureau of Export Administration, February 1991.

¹⁵³ “Imposition and Expansion of Foreign Policy Controls,” Department of Commerce, Bureau of Export Administration, August 15, 1991.

¹⁵⁴ Interview of Iain S. Baird, November 17, 1998.

¹⁵⁵ See letter from John F. Sopko, Chief Counsel for Special Matters, Department of Commerce, to Chairman Christopher Cox and Ranking Member Norm Dicks, December 14, 1998.

¹⁵⁶ Memorandum from Defense Intelligence Agency, 1992.

¹⁵⁷ “WP-11 Engine Information,” James Clauson, Jane’s Information Group, Alexandria, Virginia, June 26, 1996.

¹⁵⁸ Memorandum to Ken Weiss, Arms Control; and Disarmament Agency, 1993; and Defense Intelligence Agency.

¹⁵⁹ F. Michael Maloof, Director, Technology Security Operations, DTSA, to US Department of Commerce, August 11, 1992.

¹⁶⁰ Interview of Peter Leitner, November 24, 1998. See also letter from F. Michael Maloof, Director, Technology Security Operations, DTSA, to US Department of Commerce, August 11, 1992.

¹⁶¹ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁶² See “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC,” Memorandum from Peter Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992. See also “Garrett TFE-731-2A,” Memorandum from M. Agnello, Senior Engineer, Controls & Integrated Systems, Naval Air Warfare Center, to Charles H. Craig, Senior Engineer, Technical Directorate, DTSA/OSD, November 30, 1993; and “Engineering Analysis and Technical Policy Recommendations of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy

Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁶³ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁶⁴ Ibid.

¹⁶⁵ Ibid.

¹⁶⁶ “China Shops: Fact from Fiction,” Fact sheet attached to “The China Shop Fact Sheet,” Memorandum to Mark Kron from Iain S. Baird, Deputy Assistant Secretary for Export Administration, Department of Commerce, February 26, 1995.

¹⁶⁷ “Gas Turbine Engines,” Aviation Week & Space Technology, January 12, 1998; and “AlliedSignal TFE731,” Jane’s All the World’s Aircraft 1995-96, Jane’s Information Group, 1995.

¹⁶⁸ “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

¹⁶⁹ Letter from Martha Harris, Deputy Assistant Secretary for Export Controls, Bureau of Political Military Affairs, Department of State, to Mitchel B. Wallerstein, Deputy Assistant Secretary of Defense, Counterproliferation Policy, April 1, 1994.

¹⁷⁰ Interview of Peter Leitner, November 24, 1998.

¹⁷¹ Interview of Iain S. Baird, November 17, 1998.

¹⁷² Interview of Bruce C. Webb, December 2, 1998.

¹⁷³ For the request for records, see letter from Chairman Christopher Cox and Ranking Member Norm Dicks to William M. Daley, Secretary of Commerce, November 20, 1998. For Commerce’s response, see letter from John F. Sopko, Chief Counsel for Special Matters, Department of Commerce, to Chairman Christopher Cox and Ranking Member Norm Dicks, December 14, 1998.

¹⁷⁴ “Export of Garrett Engines to the PRC,” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992.

¹⁷⁵ Letter from Mitchel B. Wallerstein, Deputy Assistant Secretary of Defense, Counterproliferation Policy, to Martha Harris, Deputy Assistant Secretary for Export Controls, Bureau of Political Military Affairs, Department of State, March 21, 1994.

¹⁷⁶ Interview of Mitchel B. Wallerstein, November 25, 1998.

¹⁷⁷ Letter from Martha Harris, Deputy Assistant Secretary for Export Controls, Bureau of Political Military Affairs, Department of State, to Mitchel B. Wallerstein, Deputy Assistant Secretary of Defense, Counterproliferation Policy, April 1, 1994.

¹⁷⁸ "OCM 93-271/D184525-Allied Signal Aerospace Co.-Eighteen Garrett Engines," Meeting record for the Operating Committee on Export Policy, August 19, 1993.

¹⁷⁹ "Allied Signal Ends Plans to Coproduce Engines in China," Eduardo Lachica, *The Wall Street Journal*, October 27, 1995.

¹⁸⁰ Ibid.

¹⁸¹ "China Aviation Project in Doubt," *South China Morning Post*, May 15, 1996.

¹⁸² US Technology Transfers to the People's Republic of China, Kathleen Walsh, DFI International, Washington, D.C., December 1997.

¹⁸³ China's Aerospace Industry, Jane's Information Group, 1997.

¹⁸⁴ United Technologies Corporation's Responses to Written Interrogatories, November 16, 1998.

¹⁸⁵ Ibid.

White House Response to Cox Report **1 February 1999**

In his response to the Cox Report, President Clinton agreed with the need to maintain effective measures to prevent the diversion of US technology and to prevent unauthorized disclosure of sensitive military information. We also agree with the Committee's recommendation to support US high-tech competitiveness consistent with national security. This has been a longstanding premise of the Clinton Administration's technology transfer policies.

In this regard, the Administration agrees with the substance of nearly all the Committee's recommendations, many of which we have been implementing for months, and in some cases, years. We have worked cooperatively with the Committee to declassify as much of the report as possible so that the American public can be informed on these important issues, consistent with the need to protect sensitive national security and law enforcement information. The declassified report, released today, provides the Committee's detailed assessments and investigations underlying its recommendations. Although the Administration does not agree with all of the Committee's analysis, we share the Committee's objective of strengthening export controls and counterintelligence, while encouraging legitimate commerce for peaceful purposes. With regard to the specific issues raised in the report:

Security at US National Laboratories

The Administration is deeply concerned about the threat that China and other countries are seeking to acquire sensitive nuclear information from the US National Laboratories. Security at the labs has been a long-term concern, stretching back more than two decades. In 1997, the Administration recognized the need to respond to this threat with a systematic effort to strengthen counterintelligence and security at the US National Laboratories. In response, President Clinton issued a Presidential Decision Directive (PDD-61) in February 1998. This directive is the most comprehensive and

vigorous attempt ever taken to strengthen security and counterintelligence procedures at the labs. The FBI, in cooperation with DOE, is continuing its investigation into the possible source and extent of sensitive information that China may have acquired.

We welcome the Select Committee's support for PDD-61. As the President indicated in February, the Administration agrees with all of the Committee's recommendations concerning lab security, and we are carrying out these recommendations:

- The President asked the Director of Central Intelligence (DCI) to conduct a formal Intelligence Community damage assessment on China, which was reviewed by an independent panel headed by Admiral David Jeremiah. This review was completed and briefed to Congress on 21 April 1999.
- The DCI will, at the President's direction, also consider the recommendations made by Admiral Jeremiah's group on intelligence collection and resources.
- President Clinton asked the DOE to lead an interagency assessment of lab-to-lab programs with China, Russia, and other sensitive countries, which is scheduled for completion on 1 June 1999. The Administration believes that these programs serve the national security interest, but we are committed to ensuring that appropriate protections are in place to prevent compromise of classified information.
- Energy Secretary Bill Richardson is aggressively implementing PDD-61 on an expedited basis, and has been following the implementation plan that was submitted to Congress on 5 January 1999. By the end of 1999, the DOE CI program will be as good as the best in the US Government.
- Secretary Richardson has instituted a number of additional actions to improve counterintelligence security and safeguards at the National Laboratories, including in the critical area of cyber security. Secretary Richardson ordered a 14-day 'stand-down'

of all classified computers at the weapons labs, has initiated a massive reorganization of department security functions, and has greatly increased the cyber security posture at DOE.

- On 29 March 1999, the Department of Energy submitted to Congress its annual *Report Safeguards and Security at the Department of Energy Nuclear Weapons Facilities*. The report found that no nuclear material at DOE was at risk, but rated some areas 'marginal'. DOE initiated a thorough upgrade of all physical security and has committed to making all necessary upgrades so that all sites receive the highest rating by January 2000.
- The DCI, in coordination with appropriate agencies, is preparing a semi-annual report to Congress on the measures that are being taken to protect against espionage efforts by China to obtain nuclear weapons and other national security information of strategic concern.

In addition to the above steps recommended by the Select Committee, the President has requested Senator Warren Rudman, as Chairman of the bipartisan President's Foreign Intelligence Advisory Board, to evaluate security at the labs. Senator Rudman has assembled an excellent team of Board members to examine the issue. Finally, the President asked the National Counterintelligence Policy Board to recommend measures to strengthen controls over nuclear information at facilities aside from the National Laboratories that handle nuclear weapons issues.

Missile and Space Technology

The Administration agrees with the Select Committee on the need to ensure that the launch of US-manufactured civilian satellites by China or any other foreign country does not inadvertently transfer missile technology. The Department of Justice is continuing to investigate the allegations of improper transfers cited by the report, and it is inappropriate to comment on the specifics of these cases. The Administration also agrees with the

Committee on the need to establish procedures to ensure timely processing of licenses, consistent with national security.

In this regard, the Administration agrees with and is carrying out all of the Committee's recommendations concerning satellite launches:

- The Administration has implemented the provisions of the FY 1999 Defense Authorization Act by, among other things, transferring licensing for communications satellite exports from the Department of Commerce to the Department of State.
- The Department of State has developed new procedures for timely review of licenses and is increasing its licensing staff to ensure the procedures are implemented properly.

The Department of State has taken steps to ensure that the affected US companies understand and comply with the requirements of law and regulation for data that may be provided to the space insurance industry. The Department of Defense (DoD) is implementing several measures proposed by the Committee to strengthen monitoring of foreign launches. Specifically:

- DoD has established a new organization called the Space Launch Monitoring Division within the Technology Security Directorate of the Defense Threat Reduction Agency and is hiring 39 additional staff for this function. The new division fulfills the Congressional requirement in the FY 1999 National Defense Authorization Act to recruit, train, and maintain a staff dedicated to all aspects of monitoring the export of space launch and satellite technology from the United States.
- The new dedicated, professional staff in DoD will provide end-to-end monitoring of controlled space launch and satellite technologies from the first export license application through to launch and failure analyses, if necessary. The monitors will review and approve all technology-transfer control plans, and all controlled technical data

proposed for export. Monitors will participate in all technical interchange meetings and other discussions involving controlled technical data. Monitors will also deploy to launch sites as a cohesive group with expertise in space launch security operations and satellite and launch vehicle technologies.

- DoD to augment the full-time monitoring staff should that be necessary to meet temporary surges in requirements for monitoring of meetings and other activities. As well, State and DoD are requiring industry to establish electronic archiving of technical data to ensure a complete and readily accessible database of all controlled data exported as part of a satellite launch campaign.
- Training for the monitor staff is being enhanced through a program of initial and recurring training and evaluation. The training will be managed as a formal program through the Defense Threat Reduction Agency's training facilities at Kirkland Air Force Base in New Mexico. The program will encompass the complete monitoring activities outlined in the FY 1999 National Defense Authorization Act.
- Finally, DoD is examining the recommendation regarding contracting for security personnel to provide physical security at foreign launchsites. DoD looks forward to a dialogue with the appropriate congressional oversight committees on this matter.

The Administration is encouraging development of the US domestic launch industry to reduce our dependence on foreign launch services. Since 1994, the Administration has fostered the international competitiveness of the US commercial space launch industry by pursuing policies and programs aimed at developing new, lower cost US capabilities to meet both government and commercial needs. For instance, DoD is investing \$3 billion in partnership with US commercial space companies to develop and begin flying two competing families of Evolved Expendable Launch Vehicles (EELV) with a goal of

significantly reducing launch costs for government and commercial payloads.

For the longer term, NASA has committed nearly \$1 billion toward work with industry in developing and demonstrating technology for next-generation reusable launch vehicles (RLVs). NASA's goal is to reduce launch costs by a factor of 10 within 10 years. To address the shifting balance from mostly government to predominantly commercial space launches in the US, the Administration recently initiated an interagency review to assess the appropriate division of roles and responsibilities between government agencies and the US commercial space sector in managing the operation, maintenance, improvement, and modernization of the US space launch bases and ranges. Together, these measures comprise an effective strategy aimed at strengthening domestic US space launch capabilities and our industry's international competitiveness.

Domestic and International Export Policies

The Administration agrees with the Committee that the end of the Cold War and dissolution of COCOM in 1994 has complicated efforts to control transfers of militarily important dual-use goods and technology. In this regard, the Administration agrees with the Committee on the desirability of strengthening the Wassenaar Arrangement to improve international coordination and reporting on the export of militarily useful goods and technology and to prevent transfers of arms and sensitive dual-use items for military end-uses if the situation in a region or the behavior of a state is or becomes a cause of serious concern to the participating states. All Wassenaar members currently maintain national policies to prevent such transfers to Iran, Iraq, Libya, and North Korea. We are making a concerted effort in 2001 to strengthen and enhance existing transparency mechanisms and to expand restraint measures. We do not believe that other countries are prepared to accept a legally binding international regime like COCOM directed against China and we are not seeking such

a regime. We note that a COCOM-style veto could act against US interests by letting other countries block US sales to our security partners.

The Administration agrees with the Committee on the need to enact a new Export Administration Act with new penalties. We have operated for too long without updated legislation in this very important area. The Administration will work with the appropriate committees in Congress and US industry to obtain a new Export Administration Act. The Administration believes that the existing dual-use export licensing system allows adequate time for careful review of license applications and provides effective procedures to take account of national security considerations in licensing decisions.

High-Performance Computers

The Administration agrees with the Committee that we should encourage the sale of computers to China for commercial, but not military, purposes. The Administration has not licensed high-performance computers (HPCs) to China for military purposes.

As recommended by the Committee, we are reviewing the potential national security uses of various configurations of computers, the extent to which such computers are controllable, and the various consequences to the US industrial base of imposing export controls on such computers. Our target date for completing this review is May 1999.

We also agree with the Committee that we need the capability to visit US HPCs licensed for export to China to observe how they are being used. During President Clinton's visit to China in June 1998, we secured a long sought Chinese agreement to arrangements to conduct on-site visits in China to help verify the civilian use of HPCs and other dual-use technology. We have been working to expand and strengthen this arrangement. We believe that it is not possible to obtain agreement by China or any other country to a no-notice verification regime for US goods.

Chinese Technology Acquisition and Proliferation Activities

The Administration is well aware that China, like other countries, seeks to obtain sensitive US technology for military uses. We maintain strict policies prohibiting the export to China of munitions and dual-use items for military use. As recommended by the Select Committee, the FBI and CIA plan to complete their annual comprehensive threat assessment of PRC espionage by the end of May 1999, and the Inspector Generals of State, Defense, Commerce, Energy, Treasury, and CIA expect to complete their review of export controls by June 1999.

The Administration agrees with the Select Committee on the need to obtain more responsible export behavior by China. Through our policy of engagement, we believe that significant gains have been realized on this front. For example, at our initiative, China has committed not to provide assistance to unsafeguarded nuclear facilities in Pakistan or elsewhere—a commitment we believe is being observed by Beijing—terminated assistance to Iran on a project of nuclear proliferation concern and refrained from new civil and military nuclear cooperation with Iran, stopped exports of C-802 cruise missiles to Iran, and strengthened export controls over nuclear and chemical weapons related materials. China has also, with our urging, ratified the Nuclear Nonproliferation Treaty and the Chemical Weapons Convention and has signed the Comprehensive Test Ban Treaty, which are the key pillars of the international nonproliferation regime. On regional security, China has provided concrete assistance in dealing with proliferation threats in North Korea and South Asia.

The Administration agrees with the Committee that we should seek Chinese adherence to the Missile Technology Control Regime (MTCR.) In June 1998, President Jiang announced that China would actively study MTCR membership. The Administration intends to continue actively pressing the Chinese on this issue and other proliferation issues of concern.

China's High-Tech Espionage Textbook

Following is a review of an intelligence textbook in Chinese by Zhongwen, Huo, and Wang Zongxiao. *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence*. Beijing: Kexue Jishu Wenxuan Publishing Co., 1991; 361pages:

It is one thing to document on the basis of press reports, ministry decrees, and other news coming out of China about its backdoor efforts to obtain foreign defense technology. It is quite another thing to have detailed proof of these activities publicized by people who helped build China's worldwide intelligence network. Incredible as it seems, this frank account of China's longstanding program to siphon off Western military science and technology (S&T), written as a textbook for PRC intelligence officers, was sold openly in China for years.

You will not find the book in any bookstore or Chinese library today. After reporter Bruce Gilley broke the story of its publication in the 20 December 1999 issue of the *Far Eastern Economic Review* under the title "China's Spy Guide," a quiet struggle ensued between foreigners eager to procure original copies of the book and the PRC's literary custodians who wanted it out of circulation. Accordingly, some of the copies that made it out of China are missing important pages. Interested parties can find an intact book at the US Library of Congress (Q223 H86), where it had been gathering dust since August 1992.

What is unusual about this book, and the reason you cannot buy a complete copy today, is that it represents the first public acknowledgment by PRC officials of China's program to collect secret and proprietary information on foreign military hardware, especially that of the United States. The book is all the more intriguing in light of China's current media blitz to portray itself as a wellspring of indigenous R&D.

The book's authors reveal themselves as PRC intelligence officers with "more than thirty years

of experience in information collection.” Early drafts of chapters were written during their tenure as instructors at the Peoples Liberation Army’s National Defense S&T Information Center for use in training intelligence specialists. Its final version is a synthesis of practical tips on intelligence gathering with esoteric theory on the nature of information and collection, meant to serve as a reference guide for colleagues in “national defense information research.”

Although the authors complain that foreign technology collection is still in the germination stage,” it is evident from the detailed information they give that China’s intelligence apparatus was already world class a decade ago. Indeed, this is one of the few areas of “science” where China is truly competitive, as suggested by the following passage:

China’s S&T intelligence cause has already been developing for more than 30 years. As of now, we have assembled a contingent of collection workers of considerable scale in approximately 4,000 intelligence organizations throughout all of China. We have also achieved preliminary results as far as establishing S&T intelligence sources.

The authors describe an “all-China S&T intelligence system” that functions on multiple levels, including “comprehensive S&T intelligence centers” in provinces, cities, and autonomous regions. This system, they claim, was built out of recognition that traditional techniques used by scientists the world over to keep up with developments in their fields were insufficient to meet China’s special needs for economic and military construction. What China required was nothing less than a “transformation in collection work carried out with an eye to assembling the intellectual wealth of humanity.” Collection—as opposed to collaboration or creation—is seen by the authors as a necessary and cost-effective way to acquire competitive technologies.

China’s decision to invest heavily in “collection science” has borne fruit. As the authors note:

While China’s information collection work has experienced many ups and downs during these 30-odd years, it has nevertheless made outstanding contributions to the rejuvenation of the S&T intelligence cause, the invigoration of science and technology, the construction of the national economy and the build up of national defense.

The authors’ lament about “S&T collection” being in its infancy is hard to reconcile with the impact they claim pilfered technology has on national defense and with the sophistication of the intelligence organization they describe. This is evidenced in the detailed treatment they give to each stage of the intelligence process. One (80-page) chapter evaluates foreign technology sources, which turn out to be largely American.

Information collection operators should regularly peruse reference books relevant to their affairs, such as the various subscription catalogues compiled by the China National Publications Import and Export Corporation, foreign book stores and Xinhua Book Store; and such reference materials as are often used by national defense S&T information collection operators, such as the U.S. Government Report Notifications and Index, Spaceflight S&T Report, and World Conferences.

Another chapter covers in detail methods for storing and retrieving intelligence and for getting it to the right people in a timely fashion. An entire section of the book considers ways to determine consumer needs.

One of the book’s most striking aspects is the attention it gives to metrics to measure success, defined as the extent to which genuine intelligence needs are satisfied in time to make a difference. The authors address this issue comprehensively and with mathematical rigor. It is apparent that China is dead serious not only about collecting S&T intelligence but also about putting it to effective use.

Operational Collection

The authors recognize that there are limits to any collection tasking and provide three possible collection strategies. The first and most extensive is for intelligence officers to compile all information produced by a targeted source. If this is not feasible, the next best method is to collect inclusive categories of information from the target. The last strategy is to collect specifically selected information. For example, “the collection may be directed to collect all of the London International Strategic Research Institute’s research reports; or it may be directed to get the complete sets of AD reported film information or all of the NASA film reportage.” The Institute of Electrical and Electronics Engineers (IEEE) information could be the directed target of collection; or the directed collection may be a book title or some concrete leads supplied by a consumer as a “means to get the goods.” The many foreign TV signals monitored by foreign installations, or signals of foreign broadcasting stations are also directed collection.

The operational collection is not done erratically. Chinese Government entities, according to the book, provide tasking against their needs or requirements. Even if these requirements are very specific, an environment “in which the targets are not absolutely definitive, and the information that is actually wanted lie within that framework” guides the actual collection. Collection, therefore, in the authors’ opinion, is not an easy task, and “there is an aspect of randomness about it that puts a high demand on the quality and expertise of the collection operator.” They further recognize that every scrap of collected information is not necessarily useful but when a valuable indication comes to light, it will have positive results.

The authors further add that to conduct selection activities without the guidance of collection policies and plans is like trying to “cook without rice.” It can’t be done blind, nor wrested out of thin air. It must be based on frequent investigation and study with the assistance of reference materials and reference manuals.

These reference materials are diverse in form and content, and they are scattered and not easily found, and they can be rather difficult to comprehend. Collection operators rely primarily on their daily searches, discoveries, and accumulations. Most of the reference materials used today include, advertisements in periodicals and databases, publication notifications, new book and new electronic publication announcements, databases, publisher’s price lists, academic conference forecasts, critical reviews in newspapers and magazines, and verbal accounts from experts and students.

To promote sales and expand distribution, domestic and foreign media sources periodically or randomly publish reference books that consumers use for reference in the process of making selections. They include subscription catalogues, publication catalogues, new book weeklies, and cumulative book lists. Although the primary purpose of reference book search and book list databases is for researchers to investigate and find materials, it is a convenient way for information collection operators to find leads to information sources.

More than 80 percent of all consumer requirements can be satisfied by overt information; therefore, if all of the information collected through whatever channels by all elements were put together to form a consultation network of shared information, under existing conditions researchers requirements could—for the most part—be satisfied.

Open Sources

One of the most startling revelations in *Sources and Techniques* is the extent to which the Chinese military and defense industries rely on open-source information, particularly US and British, for weapons modernization. According to the spying manual, more than 80 percent of all Chinese spying focuses on open-source material obtained from government and private-sector information. The remaining 20 percent of the information is gathered through illicit means, including eliciting information from scientists at meetings, through

documents supplied by agents, or through electronic eavesdropping.

This fact contrasts with the Cox Report's emphasis on China's use of covert methods to obtain military secrets. It also adds a critical dimension to our understanding of Chinese collection techniques as focusing on cooperative agreements and the exploitation of overseas scientists.

Astronautics (AIAA) publications and Department of Energy reports, particularly nuclear power and weapons-related studies, "continue to get a great deal of attention from those engaged in national defense S&T work" and are regarded as an "intelligence source of great value." US military standards as revealed in public bid specifications, drawings, and handbooks receive detailed scrutiny.

The authors concede that collecting national defense S&T information is difficult because of security classifications, but not impossible. As they put it:

There are no walls which completely block the wind, nor is absolute secrecy achievable. Invariably there will be numerous open situations in which things are revealed, either in a tangible or intangible form. By picking up here and there among the vast amount of public materials and accumulating information a drop at a time, often it is possible basically to reveal the outlines of some secret intelligence, and this is particularly true in the case of Western countries.

As an example of the payoff for diligence, the authors cite a program to declassify documents on thermonuclear weapons at a US national laboratory in the 1970s that resulted in 19,400 documents being declassified in error. The book explains:

This incident tells us that, on the one hand, absolute secrecy is not attainable, while on the other hand, there is a random element involved in the discovery of secret intelligence sources, and to turn this randomness into inevitability, it is

necessary that there be those who monitor some sectors and areas with regularity and vigilance.

The authors state unequivocally that Western scientific journals "are the first choice of rank-and-file S&T personnel as well as intelligence researchers." They then provide the results of a "core periodical survey" run by China's National Defense S&T Intelligence Center, which lists the 56 most popular defense technology journals, including 33 from the United States and 12 more from the United Kingdom. Another list of 80 journals included 43 titles published in the United States, the most popular ones dealing with aerospace.

Conferences

Information collection is conducted through personal contacts, as in attending academic exchange conferences, technical exchange conferences, planning, demonstration, and appraisal meetings and through discussions between individuals. This is the procedure commonly used for collecting verbal information, but it is not limited to verbal information. Participation in consultative activities is also a person to person exchange procedure for collecting information.

The Chinese manual notes, "It is also necessary to stress that there is still 20 percent or less of our intelligence that must come through the collection of information using special means, such as reconnaissance satellites, electronic eavesdropping, and the activities of special agents (purchasing or stealing) . . ."

So why did China, a country not known for its willingness to share state secrets, allow such a book to be published? Mr. Gilley in his *Far Eastern Economic Review* article attributed the release of *Sources and Techniques* to an "oversight," adding that it could not be published in the atmosphere that prevails today. True enough. But to someone familiar with the psychology of Chinese technology transfer there is another explanation that is both

more facile and disconcerting. China's commitment to expropriating foreign technology is so much a part of its R&D culture that the book's authors simply took acceptance of this behavior for granted.

Support for this hypothesis is found in the regularity with which tech-transfer schemes are reported in China's "open" press, particularly as they involve the targeting by Beijing of ethnic Chinese scientists overseas. It is also evident in the authors' demand that collection of foreign S&T intelligence be treated as a "science" in its own right. It would seem that China's claim to innovation, as it were, is not entirely disingenuous, at least as it applies to intelligence collection.

Old-Fashioned Espionage

Regarding espionage, the report states: "It is also necessary to stress that there is still 20 percent or less of our intelligence that must come through the collection of information using special means, such as reconnaissance satellites, electronic eavesdropping and the activities of special agents purchasing or stealing, etc."

The report further states that direct contact with scientists and other spying targets "is the procedure commonly used for collecting verbal information, but it is not limited to verbal communications. Participation in consultative activities is also a person-to-person exchange procedure for collecting information."

The information is gathered from people and institutions, including government agencies, research offices, corporate enterprises, colleges and universities, libraries, and information offices.

Report on the Investigation of Espionage Allegations Against Dr. Wen Ho Lee

8 March 2000

Summary

While the full impact of the errors and omissions by the Department of Energy (DOE) and the Department of Justice (DOJ)—including the Federal Bureau of Investigation (FBI)—in the investigation of Dr. Wen Ho Lee requires reading the full report, this summary covers some of the highlights.

The importance of Dr. Lee's case was articulated at his bail hearing on 13 December 1999 when Dr. Stephen Younger, Assistant Laboratory Director for Nuclear Weapons at Los Alamos, testified:

These codes, and their associated databases, and the input file, combined with someone that knew how to use them, could, in my opinion, in the wrong hands, change the global strategic balance.¹ (Emphasis added)

Younger further noted about the codes Dr. Lee mishandled:

They enable the possessor to design the only objects that could result in the military defeat of America's conventional forces . . . They represent the gravest possible security risk to . . . the supreme national interest.² (Emphasis added) A "military defeat of America's conventional forces" and "the gravest possible security risk to . . . the supreme national interest" constitute threats of obvious enormous importance.

It would be hard—realistically impossible—to pose more severe risks to US national security.

Although the FBI knew that Dr. Lee had access to highly classified information, had repeated contacts with the PRC scientists, and lied about his activities, the FBI investigation was inept. In December 1982, Dr. Lee called a former employee of Lawrence Livermore National Laboratory (LLNL).

Although the Subcommittee's inquiry into the handling of the Dr. Wen Ho Lee investigation is not completed, important conclusions have been reached that require Congressional consideration of remedial legislation at the earliest possible time.

The purpose of counterintelligence is to identify suspicious conduct and then pursue an investigation to prevent or minimize access by foreign agents to our secrets. The investigation of Dr. Lee since 1982 has been characterized by a series of errors and omissions by the Department of Energy and the Department of Justice, including the FBI, which have permitted Dr. Lee to threaten US supremacy by putting at risk information that could change the "global strategic balance." This interim report will describe and discuss some of those errors and omissions and suggest remedial legislation.

Dr. Wen Ho Lee was investigated on multiple occasions during a 17-year period, but none of these investigations—or the security measures in place at Los Alamos—came close to discovering and preventing Dr. Lee from putting the national security at risk by placing highly classified nuclear secrets on an unsecured system where they could easily be accessed by even unsophisticated hackers.³ Given all the indicators that were present, it is difficult to comprehend how officials entrusted with the responsibility for protecting our national security could have failed to discover what was really happening with Dr. Lee.

The Investigation of 1982-84

Dr. Wen Ho Lee was born in Nantou, Taiwan, in 1939. After graduating from Texas A&M University with a doctorate in 1969, he became a US citizen in 1974 and began working at Los Alamos National Laboratory in applied mathematics and fluid dynamics in 1978.⁴ The FBI first became concerned about Dr. Lee as a result of contacts he made with a suspected PRC intelligence agent in the early 1980s. On 3 December 1982, Dr. Lee called a former employee of Lawrence Livermore National Laboratory

(LLNL) who was suspected of passing classified information to the Peoples Republic of China (PRC). This call was intercepted pursuant to a Foreign Intelligence Surveillance Act (FISA) court-authorized wiretap in another FBI espionage investigation. After introducing himself, Dr. Lee stated that he had heard about the Lawrence Livermore scientist's "matter" and that Lee thought he could find out who had "squealed" on the employee.⁵ On the basis of the intercepted phone call, the FBI opened an espionage investigation on Dr. Lee.

For the next several months, the FBI investigated Dr. Lee with much of the work being done under the guise of the periodic reinvestigation required for individuals with security clearances. On 9 November 1983, the FBI interviewed Dr. Lee. Before being informed that the FBI had intercepted his call to the Lawrence Livermore employee, Lee stated that he had never attempted to contact the employee, did not know the employee, and had not initiated any telephone calls to him. These representations were patently false.⁶ During the course of this interview, Dr. Lee offered to assist the FBI with its investigation of the other scientist.

On 20 December 1983, the FBI again interviewed Dr. Lee,⁷ this time in California. During this interview, Lee explained that he had been in contact with Taiwanese nuclear researchers since 1977 or 1978, had done consulting work for them, and had sent some information that was not classified but that should have been cleared with DOE officials. He tried to explain that he had contacted the subject of the other investigation because he thought this other scientist was in trouble for doing the same thing that Lee had been doing for Taiwan.⁸ After this interview, the FBI sent Dr. Lee to meet with the espionage suspect. On the record currently available, that meeting did not produce anything.

On 24 January 1984, Dr. Lee took an FBI polygraph examination, which included questions about passing classified information to any foreign government, Lee's contacts with the Taiwanese Embassy, and his contacts with the LLNL scientist. Although the FBI has subsequently contended

that Dr. Lee's answers on this polygraph were satisfactory,⁹ there remained important reasons to continue the investigation. His suspicious conduct in contacting the Lawrence Livermore scientist and then lying about it, the nature of the documents that he was sending to the Taiwanese Embassy, and the status of the person to whom he was sending those documents were potential danger signals. Although not classified, the documents Dr. Lee was passing to Taiwan's Coordination Council of North America were subject to Nuclear Regulatory Commission export controls. They were specifically stamped "no foreign dissemination." According to the testimony of FBI Special Agent Robert Messemer at a special hearing on 29 December 1999, FBI files also contain evidence of other "misrepresentations" that Dr. Lee made to the FBI during the period 1983-84 that have raised "grave and serious concerns" about Dr. Lee's truthfulness. For security reasons, these matters cannot be further detailed.¹⁰ Notwithstanding these reasons for continuing the investigation, the FBI closed its initial investigation of Lee on 12 March 1984.¹¹

During the course of the 1982-84 investigation, it was clear that, by virtue of his work assignment and access to top nuclear secrets, Dr. Lee was in a position to do considerable damage to the national security. Thus, suspicions of espionage or a lack of trustworthiness should have been treated with great concern. On the state of the record, consideration should have been given to suspending his access to classified information, and, at a minimum, an intensified investigation should have been pursued. Instead, the FBI permitted him to stay in place, which enabled him to undertake a course of conduct—years later—leading to his potential to change the global strategic balance.

The 1982-84 investigation of Dr. Lee represents a missed opportunity to protect the nation's secrets. Had the matter been handled properly, Dr. Lee's clearance and access would most likely have been removed long ago before he was able to put the global strategic balance at risk.

The Investigation of Dr. Lee From 1994 to 2 November 1995

This investigation of Dr. Lee was initiated based on the discovery that he was well acquainted with a high-ranking Chinese nuclear scientist who visited Los Alamos as part of a delegation in 1994.¹² Dr. Lee had never reported meeting this scientist, which he was required to do by DOE regulations, so his relationship with this person aroused the FBI's concern. Unclassified sources have reported that Dr. Lee was greeted by "a leading scientist in China's nuclear weapons program who then made it clear to others in the meeting that Lee had been helpful to China's nuclear program."¹³ In concert with the 1982-84 investigation, Dr. Lee's undisclosed relationship with this top Chinese nuclear scientist should have alerted the FBI and the DOE that it was imperative to do an intensified investigation and reconsideration of his access to classified information. Instead, this FBI investigation was deferred on 2 November 1995 because Dr. Lee was by then emerging as a central figure in the Department of Energy's Administrative Inquiry (AI), which was developed by a DOE counterintelligence expert in concert with a seasoned FBI agent who had been assigned to DOE for the purposes of the inquiry. The DOE AI was given the code name Kindred Spirit.¹⁴ The investigation of Dr. Lee was essentially dormant from November 1995 until May 1996, when the FBI received the results of the DOE AI and opened a new investigation of Dr. Lee on 30 May 1996.

It is difficult to understand why the FBI suspended the investigation in 1995, even to wait for the Kindred Spirit AI, when the issues that gave rise to the 1994-95 investigation remained valid and unrelated to the Kindred Spirit investigation. The key elements of the 1994-95 investigation are described in the Letterhead Memorandum (LHM) of 1997, which was prepared to support the request for a FISA search warrant. Specifically, the LHM describes the unreported contact with the top nuclear scientist,¹⁵ and it makes reference to the "PRC using certain computational codes . . . which were later identified as something that [Lee] had unique access to."¹⁶ Finally, the LHM states that,

“the Director subsequently learned that Lee Wen Ho had worked on legacy codes.”¹⁷ Given these serious allegations, it was a serious error to allow the investigation to wait for several months while the DOE AI was being completed. This deferral needlessly delayed the investigation and left important issues unresolved.

In addition to information known to the FBI, which required further intensified investigation rather than the deferred investigation on 2 November 1995, the DOE was incredibly lax in failing to understand and pursue obvious evidence that Dr. Lee was downloading large quantities of classified information to an unclassified system. The sheer volume of Dr. Lee’s downloading showed up on a DOE report in 1993.¹⁸ Cheryl Wampler, from the Los Alamos computer office of LLNL, has testified that the NADIR system—Network Anomaly Detection and Intrusion Recording—flagged Dr. Lee’s massive downloading in 1993.¹⁹ This system is specifically designed to create profiles of scientists’ daily computer usage so it can detect unusual behaviors. A DOE official with direct knowledge of Lee’s suspicious activity failed to act on it or to tell DOE counterintelligence personnel or the FBI. On the basis of its design, the NADIR system would have continued to flag Dr. Lee’s computer activities in 1994 as being unusual, but no one from DOE took any action to investigate what was going on.²⁰ Also, Dr. Lee’s downloading of classified information was not mentioned to the FBI or DOE’s counterintelligence personnel.

Had DOE transmitted this information to the FBI, and had the FBI acted on it, Dr. Lee could have and should have been stopped in his tracks in 1994 on these indicators of downloading. The full extent of the importance of the information that Dr. Lee was putting at risk through his downloading was encapsulated in a document the government filed in December 1999 as part of the criminal action against Dr. Lee:

[I]n 1993 and 1994, Lee knowingly assembled 19 collections of files, called tape archive (TAR) files, containing Secret and Confidential Restricted Data relating to atomic weapon

*research, design, construction, and testing. Lee gathered and collected information from the secure, classified LANL computer system, moved it to an unsecured, “open” computer, and then later downloaded 17 of the 19 classified TAR files to nine portable computer tapes.*²¹

These files, which amounted to more than 806 megabytes, contained information that could do vast damage to the national security.

The end result of these missteps and lack of communication was that, during some of the very time that the FBI had an espionage investigation open on Dr. Lee resulting from his unreported contacts with a top Chinese scientist and the realization that the Chinese were using codes to which Dr. Lee had unique access, DOE computer personnel were being warned by the NADIR system that Dr. Lee was moving suspiciously large amounts of information around but were ignoring those warnings and were not passing them on to the FBI.

The near-perfect correlation between the allegations, which began the 1994-95 investigation and Dr. Lee’s computer activities, is stunning. The codes the Chinese were known to be using were computer codes, yet FBI and DOE counterintelligence officials never managed to discover these massive file transfers. Where, if not on his computer, were they looking? And, as for the lab computer personnel who saw but ignored the NADIR reports, what possible explanation can there be for a failure to conduct even the most minimal investigation?

The Investigation Renewed—30 May 1996 to 12 August 1997

As noted previously, the investigation of Dr. Lee was dormant from 2 November 1995 until 30 May 1996.

In 1995, DOE scientists received information that raised the possibility that the Chinese had made significant technological advancements in warhead design. The now infamous “walk-in”

document was added to the equation in the summer of 1995. The walk-in document, coupled with concerns raised from a string of Chinese nuclear tests, led to the formal establishment of a DOE AI on 28 September 1995. As noted previously, at DOE's request, a senior FBI special agent was assigned to work this inquiry jointly with a DOE counterintelligence officer. This AI was presented to the FBI on 28 May 1996, and the FBI reopened its investigation of Dr. Lee on 30 May 1996.

The walk-in document is central to the Kindred Spirit investigation so it should be described in the greatest detail consistent with classification concerns. This document, dated 1988, is said to lay out China's nuclear modernization plan for Beijing's First Ministry of Machine Building, which is responsible for making missiles and nose cones.²² The 74-page document contains dozens of facts about US warheads, mostly in a two-page chart. On one side of the chart are various US Air Force and US Navy warheads, including some older bombs as well as the W-80 warhead (cruise missiles), the W-87 (Minuteman III), and the W-88 (Trident II).²³ Among the most important items of information in the walk-in document are details about the W-88 warhead.

The *Cox Committee Report* provides the following description and assessment of the walk-in document:

In 1995, a "walk-in" approached the Central Intelligence Agency outside of the PRC and provided an official PRC document classified "Secret" that contained design information on the W-88 Trident D-5 warhead, the most modern in the US arsenal, as well as technical information concerning other thermonuclear warheads.

The CIA later determined that the "walk-in" was directed by the PRC intelligence services. Nonetheless, the CIA and other Intelligence Community analysts that reviewed the document concluded that it contained US thermonuclear warhead design information.

The "walk-in" document recognized that the US nuclear warheads represented the state-of-the-art against which PRC thermonuclear warheads should be measured.

Over the following months, an assessment of the information in the document was conducted by a multidisciplinary group from the US government, including the Department of Energy and scientists from the US national weapons laboratories.²⁴

The Cox Committee's view that the Chinese had obtained sensitive design information about US thermonuclear warheads is bolstered by the June 1999 report of the President's Foreign Intelligence Advisory Board, which states that the walk-in document:

Unquestionably contains some information that is still highly sensitive, including descriptions, in varying degrees of specificity, of the technical characteristics of seven US thermonuclear warheads.²⁵

When the FBI received notice that the source of the walk-in document was under the control of PRC intelligence services, however, the Kindred Spirit investigation was actually halted for a time, from 31 July 1996 until 20 August 1996. Even when it was restarted, it was not pursued with particular vigor in the latter part of 1996.

It is surprising that the investigation was halted, even for a few weeks, since it was conclusive that the walk-in document did contain important classified information, which had somehow fallen into the hands of a foreign power. The *Cox Committee Report* and the President's Foreign Intelligence Advisory Board have recently reconfirmed that the walk-in document was proof that the Chinese had obtained sensitive nuclear information, but there should never have been any doubt on the part of the FBI about that question in the summer of 1996. Moreover, the information, which led to the 1994-95 investigation, was no less valid because of any doubts about the walk-in document or even the Kindred Spirit Administrative Inquiry itself.

From 1996 until 1997 the DOE and FBI investigation was characterized by additional inexplicable lapses. For example, in November 1996, the FBI asked DOE counterintelligence team leader Terry Craig for access to Dr. Lee's computer. Although Mr. Craig apparently did not know it until 1999, Dr. Lee had signed a consent-to-monitor waiver²⁶ on 19 April 1995. The relevant portion of the waiver states:

*WARNING: To protect the LAN [local area network] systems from unauthorized use and to ensure that the systems are functioning properly, activities on these systems are monitored and recorded and subject to audit. Use of these systems is expressed consent to such monitoring and recording. Any unauthorized access or use of this LAN is prohibited and could be subject to criminal and civil penalties.*²⁷

Moreover, the computer that Dr. Lee used apparently also had a banner, which had information that may have constituted sufficient notice to give the FBI access to its contents. And, finally, the Los Alamos National Laboratories (LANL) computer-use policy gave authorities the ability to search computers to prevent waste, fraud, and abuse.²⁸ As noted in the press release accompanying the Department of Energy Inspector General's Report of 12 August 1999, Mr. Craig's "failure to conduct a diligent search deprived the FBI of relevant and potentially vital information."²⁹ Had the FBI National Security Law Unit (NSLU) been given the opportunity to review these facts, it may well have concluded that no FISA warrant was necessary to conduct a preliminary investigation of Dr. Lee's computer. More important, records from the DOE monitoring systems like NADIR could almost certainly have been reviewed without a FISA warrant. Had these records been searched, Dr. Lee's unauthorized downloading would have been found nearly three years earlier. Unfortunately, through the failures of both DOE and FBI personnel, this critical information never reached FBI Headquarters, and the NSLU decided that Dr. Lee's computer could not be searched without a FISA warrant.³⁰ Thus, a

critical opportunity was lost to find and remove from an unsecured system information that could alter the global strategic balance.

Nonetheless, the FBI developed an adequate factual basis for the issuance of a FISA warrant. Senators Thompson and Lieberman of the Senate Committee on Governmental Affairs cogently summarized the information developed by the FBI to support its FISA application in 1997 in the special statement of 5 August 1999:³¹

1. DOE counterintelligence and weapons experts had concluded that there was a great probability that the W-88 information had been compromised between 1984 and 1988 at the nuclear weapons division of the Los Alamos laboratory.
2. It was standard PRC intelligence tradecraft to focus particularly upon targeting and recruitment of ethnic Chinese living in foreign countries (for example, Chinese-Americans).
3. It is common in PRC intelligence tradecraft to use academic delegations—rather than traditional intelligence officers—to collect information on science-related topics. It was, in fact, standard PRC intelligence tradecraft to use scientific delegations to identify and target scientists working at restricted US facilities such as LANL, since they "have better access than PRC intelligence personnel to scientists and other counterparts at the United States National Laboratories."
4. Sylvia Lee, wife of Wen Ho Lee, had extremely close contacts with visiting Chinese scientific delegations. Sylvia Lee, in fact, had volunteered to act as hostess for visiting Chinese scientific delegations at LANL when such visits first began in 1980 and had apparently had more extensive contacts and closer relationships with these delegations than anyone else at the laboratory. On one occasion, moreover, Wen Ho Lee had himself aggressively sought involvement with a visiting Chinese scientific

-
- delegation, insisting upon acting as an interpreter for the group despite his inability to perform this function very effectively.
5. Sylvia Lee was involuntarily terminated at LANL during a reduction in force in 1995. Her personnel file indicated incidents of security violations and threats she allegedly made against coworkers.
 6. In 1986, Wen Ho Lee and his wife traveled to China on LANL business to deliver a paper on hydrodynamics³² to a symposium in Beijing. He visited the Chinese laboratory—the Institute for Applied Physics and Computational Mathematics (IAPCM)—that designs the PRC’s nuclear weapons.
 7. The Lees visited the PRC—and IAPCM—on LANL business again in 1988.
 8. It was standard PRC intelligence tradecraft, when targeting ethnic Chinese living overseas, to encourage travel to the “homeland”—particularly where visits to ancestral villages and/or old family members could be arranged—as a way of trying to dilute loyalty to other countries and encouraging solidarity with the authorities in Beijing.
 9. The Lees took vacation time to travel elsewhere in China during their two trips to China in 1986 and 1988.
 10. The FBI also learned of the Lees’ purchase of unknown goods or services from a travel agent in Hong Kong while on a trip to that colony and to Taiwan in 1992. On the basis of the record, the FBI determined that there was reason to believe that this payment might have been for tickets for an unreported sidetrip across the border into the PRC to Beijing.
 11. Although Wen Ho Lee had visited IAPCM in both 1986 and 1988 and had filed “contact reports” claiming to recount all of the Chinese scientists he met there, he had failed to disclose his relationship with the PRC scientist who visited LANL in 1994.
 12. Wen Ho Lee worked on specialized computer codes at Los Alamos—so-called legacy codes related to nuclear testing data—that were a particular target for Chinese intelligence.
 13. The FBI learned that during a visit to Los Alamos by scientists from IAPCM, Lee had discussed certain unclassified hydrodynamic computer codes with the Chinese delegation. It was reported that Lee had helped the Chinese scientists with their codes by providing software and calculations relating to hydrodynamics.
 14. In 1997, Lee had requested permission to hire a graduate student, a Chinese national, to help him with work on “Lagrangian codes” at LANL. When the FBI evaluated this request, investigators were told by laboratory officials that there was no such thing as an unclassified Lagrangian code, which describes certain hydrodynamic processes and are used to model some aspects of nuclear weapons testing.
 15. In 1984, the FBI questioned Wen Ho Lee about his contact in 1982 with a US scientist at another DOE nuclear weapons laboratory who was under investigation.
 16. When questioned about this contact, Lee gave deceptive answers. After offering further explanations, Lee took a polygraph, claiming that he had been concerned only with this other scientist’s alleged passing of unclassified information to a foreign government against DOE and Nuclear Regulatory Commission regulations—something that Lee himself admitted doing. (As previously noted, the FBI closed this investigation of Lee in 1984.)
 17. The FBI, as noted above, had begun another investigation into Lee in the early 1990s, before the W-88 design information compromise came to light. This investigation was based upon an

FBI investigative lead that Lee had provided significant assistance to the PRC.

18. The FBI obtained a copy of a note on IAPCM letterhead dated 1987 listing three LANL reports by their laboratory publication number. On this note, in English, was a handwritten comment to “Linda” saying “[t]he Deputy Director of this Institute asked [for] these paper[s]. His name is Dr. Zheng Shaotang. Please check if they are unclassified and send to them. Thanks a lot. Sylvia Lee.”

The FBI request was worked into a draft FISA application by Mr. David Ryan, a line attorney from the Department of Justice’s Office of Intelligence Policy and Review (OIPR) with considerable experience in FISA matters. It was then reviewed by Mr. Allan Kornblum, as Deputy Counsel for Intelligence Operations, and finally, by Mr. Gerald Schroeder, Acting Counsel, OIPR.³³ As is well known by now, the OIPR did not agree to forward the FISA application, and yet another opportunity to discover what Dr. Lee was up to was lost.

The Department of Justice should have taken the FBI’s request for a FISA warrant on Dr. Lee to the court on 12 August 1997.

Attorney General Janet Reno testified about this case before the Senate Judiciary Committee on 8 June 1999. A redacted version of her testimony was released on 21 December 1999. The transcript makes it clear that the Department of Justice should have agreed to go forward with the search warrant for surveillance of Dr. Wen Ho Lee under the Foreign Intelligence Surveillance Act when the FBI made the request in 1997.

In evaluating the sufficiency of the FBI’s statement of probable cause, the Attorney General and the Department of Justice failed to follow the standards of the Supreme Court of the United States that the requirements for “domestic surveillance may be less precise than that directed against more conventional types of crime.” In *United States v. U.S. District Court* 407 U.S. 297, 322-23 (1972) the Court held:

We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime” . . . the focus of domestic surveillance may be less precise than that directed against more conventional types of crime Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. [emphasis added]

Even where domestic surveillance is not involved, the Supreme Court has held that the first focus is upon the governmental interest involved in determining whether constitutional standards are met. In *Camera v. Municipal Court of the City and County of San Francisco*, 387 U.S. 523, 534-539, (1967), the Supreme Court said:

In cases in which the Fourth Amendment requires that a warrant to search be obtained, “probable cause” is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness. To apply this standard, it is obviously necessary first to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen . . . [emphasis added]

Unfortunately, there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion, which the search entails The warrant procedure is designed to guarantee that a decision to search private property is justified by a reasonable governmental interest. But reasonableness is still the ultimate standard. If a valid public interest justifies the intrusion contemplated, then there is probable cause to issue a suitably restricted search warrant.

Where the Court allowed inspections *in camera* without probable cause that a particular dwelling contained violations, it is obvious that even more latitude would be constitutionally permissible where national security is an issue, and millions of American lives may be at stake. Even under the erroneous, unduly high standard applied by the Department of Justice, however, the FBI's statement of probable cause was sufficient to activate the FISA warrant.

FBI Director Freeh correctly concluded that probable cause existed for the issuance of the FISA warrant. At the hearing on 8 June, Attorney General Reno stated her belief that there had not been a sufficient showing of probable cause but conceded that FBI Director Freeh, a former Federal judge, concluded that probable cause existed as a matter of law.³⁴

The Department of Justice applied a clearly erroneous standard to determine whether probable cause existed. As noted in the transcript of Attorney General Reno's testimony:

*On 8-12-97 Mr. Allan Kornblum of OIPR advised that he could not send our (the FBI) application forward for those reasons. We had not shown that subjects were the ones who passed the W-88 [design information] to the PRC, and we had little to show that they were presently engaged in clandestine intelligence activities.*³⁵

It is obviously not necessary to have a showing that the subjects were the ones who passed W-88 design information to the PRC. That would be the standard for establishing guilt at a trial, which is a far higher standard than establishing probable cause for the issuance of a search warrant. Attorney General Reno contended that other people, actually a relatively small number of people, would have to be ruled out as the ones who passed W-88 design information to the PRC before probable cause would be established for issuance of the FISA warrant on Dr. Lee. That, again, is the standard for conviction at trial instead of establishing probable cause for the issuance of a search warrant. For

some inexplicable reason, the Department of Justice has insisted on redacting the exact number of people who were situated similarly to Dr. Lee. However, it is apparent from the Kornblum statement that the wrong standard was applied, "that subjects were the ones that passed the W-88 [design information] to the PRC."³⁶

DOJ was also wrong when Mr. Kornblum concluded that: "We had little to show that they were presently engaged in clandestine intelligence activities."³⁷ There is substantial evidence that Dr. Lee's relevant activities continued from the 1980s to 1992, 1994, and 1997 as noted above. When FBI Assistant Director John Lewis met with Attorney General Reno on 20 August 1997 to ask about the issuance of the FISA warrant, Attorney General Reno delegated the matter to Mr. Daniel Seikaly, former Director, DOJ Executive Office for National Security, and she had nothing more to do with the matter. Mr. Seikaly completed his review by late August or early September and communicated his results to the FBI through Mr. Kornblum. As Mr. Seikaly has testified, this was the first time he had ever worked on a FISA request, and he was not "a FISA expert." It was not surprising then that Seikaly applied the wrong standard for a FISA application:

*We can't do it (a FISA wiretap) unless there was probable cause to believe that that facility, their home, is being used or about to be used by them as agents of a foreign power.*³⁸

Mr. Seikaly applied the standard from the typical criminal warrant as opposed to a FISA warrant. 18 U.S.C. 2518, governing criminal wiretaps, allows surveillance where there is:

Probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted, are being used, or are about to be used in connection with the commission of such offense. [emphasis added]

This criminal standard specifically requires that the facility be used in the "commission of such offense." FISA, however, contains no such

requirement, and 50 U.S.C. 1805 (Section 105 of FISA) states that a warrant shall be issued if there is probable cause to believe that:

Each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.

There is no requirement in this FISA language that the facility is being used in the commission of an offense.

Attorney General Reno demonstrated unfamiliarity with technical requirements of Section 1802 versus Section 1804. She was questioned about the higher standard under 1802 than 1804: “It seems the statutory scheme is a lot tougher on 1802 on its face.”³⁹

Attorney General Reno replied, “Well I don’t know. I’ve got to make a finding that under 1804, that it satisfies the requirement and criteria—and requirement of such application as set forth in the chapter, and it’s fairly detailed.”⁴⁰

When further questioned about her interpretation on 1802 and 1804, Attorney General Reno indicated a lack of familiarity with these provisions, saying:

*Since I did not address this, let me ask Ms. Townsend who heads the office of policy review to address it for you in this context and then I will . . .*⁴¹

As noted in the record, the offer to let Ms. Townsend answer the question was rejected in the interest of getting the Attorney General’s view on this important matter rather than that of a subordinate.

The lack of communication between the Attorney General and the Director of the FBI on a matter of such grave importance is troubling. As noted previously, Director Freeh sent John Lewis, Assistant FBI Director for National Security, to discuss this matter with the Attorney General on

20 August 1996. However, when the request for a review of the matter did not lead to the forwarding of the FISA application to the court, Director Freeh did not further press the issue. Attorney General Reno conceded that she did not follow up on the Wen Ho Lee matter. During the hearing on 8 June, Senator Sessions asked, “Did your staff convey to you that they had once again denied this matter?”⁴²

Attorney General Reno replied, “No, they had not.”⁴³

The hearing of 8 June 1999 also included a discussion as to whether FBI Director Freeh should have personally brought the matter again to Attorney General Reno. The Attorney General replied that she did not “complain” about FBI Director Freeh’s not doing so and stated, “I hold myself responsible for it.”⁴⁴ Attorney General Reno conceded the seriousness of the case, stating, “I don’t think the FBI had to convey to the attorneys the seriousness of it. I think anytime you are faced with facts like this it is extremely serious.”⁴⁵

In the context of this serious case, it would have been expected that Attorney General Reno would have agreed with FBI Director Freeh that the FISA warrant should have been issued. In her testimony, she conceded that, if some 300 lives were at stake on a 747, she would take a chance, testifying, “My chance that I take if I illegally search somebody, if I save 300 lives on a 747, I’d take it.”⁴⁶

In that context, with the potential for the PRC obtaining US secrets on nuclear warheads putting at risk millions of Americans, it would have been expected that the Attorney General would find a balance in favor of moving forward with the FISA warrant. As demonstrated by her testimony, Attorney General Reno sought, at every turn, to minimize the FBI’s statement of probable cause. On the issue of Dr. Lee’s opportunity to have visited Beijing while he was in Hong Kong and incurred additional travel costs of the approximate expense of traveling to Beijing, the Attorney General said that, “an unexplained travel voucher in Hong Kong does not lead me to the conclusion

that someone went to Beijing any more than they went to Taipei.”⁴⁷

It might well be reasonable for a factfinder to conclude that Dr. Lee did not go to Beijing; but, certainly, his proximity to Beijing, the opportunity to visit there, and his inclination for having done so in the past would at least provide some “weight” in assessing probable cause. But the Attorney General dismissed those factors as having no weight even on the issue of probable cause, testifying, “I don’t find any weight when I don’t know where the person went.”⁴⁸ Of course, it is not known “where the person went.” If that fact had been established, it would have been beyond the realm of “probable cause.” Such summary dismissal by the Attorney General on a matter involving national security is inappropriate given the circumstances. In other legal contexts, opportunity and inclination are sufficient to cause an inference of certain conduct as a matter of law.

The importance of DOJ’s erroneous interpretation of the law in this case, which resulted in the FISA rejection, should not be underestimated. Had this application for a FISA warrant been submitted to the court, it doubtless would have been approved. DOJ officials reported that approximately 800 FISA warrants were issued each year with no one remembering any occasion when the court rejected an application.

Had the FBI obtained the FISA search warrant, it might have had a material effect on the investigation and criminal charging of Dr. Lee. Given the serious mistakes that had been made by the FBI prior to 1997, there is no guarantee that a FISA warrant would have led to a successful conclusion to the investigation, but the failure to issue a warrant clearly had an adverse impact on the case. Certainly, Dr. Lee would have been removed from a very sensitive job at least 18 months earlier, and the probabilities are high that significant additional incriminating evidence could have been found had Dr. Lee not had the opportunity to download the codes and conceal his taking of sensitive information.

To put the FISA rejection of 1997 in perspective, consider that the open network to which Dr. Lee had transferred the legacy codes was “linked to the Internet and e-mail, a system that had been attacked several times by hackers.”⁴⁹ Although we do not know the exact figures for the number of times that it was accessed, it has been reported that between October 1997 and June 1998 alone, “there were more than 300 foreign attacks on the Energy Department’s unclassified systems, where Mr. Lee had downloaded the secrets of the US nuclear arsenal.”⁵⁰

Consider also the following from a government filing of 23 December 1999 in the criminal case against Dr. Lee:

*... in 1997 Lee downloaded directly from the classified system to a tenth portable computer tape a current nuclear weapons design code and its auxiliary libraries and utility codes.*⁵¹

This direct downloading had been made possible by Los Alamos computer managers who made Lee’s file transfers “easier in the mid-1990s by putting a tape drive on Lee’s classified computer.”⁵² As incomprehensible as it seems, despite the fact that Dr. Lee was the prime suspect in an ongoing espionage investigation, and despite plans to restrict his access to classified information to limit any damage he might do, DOE computer personnel installed a tape drive on his computer that made it possible for him to directly download the nation’s top nuclear secrets. An important aim of surveillance under the FISA statute is to determine whether foreign intelligence services are getting access to our classified national security information. Despite what we know about Dr. Lee’s activities—and regardless of whether a jury ever finds that his acts were criminal—there should be no doubt that transferring classified information to an unclassified computer system and making unauthorized tape copies of that information created a substantial opportunity for foreign intelligence services to access that information.

Investigation From 12 August 1997 to 23 December 1998

Notwithstanding the serious evidence against Dr. Lee on matters of great national security importance, the FBI investigation languished for 16 months—from August 1997 until December 1998—with the Department of Energy permitting Dr. Lee to continue on the job with access to classified information.

After OIPR's decision in August 1997 not to forward the FISA application, FBI Director Louis Freeh met with Deputy Energy Secretary Elizabeth Moler to tell her that there was no longer any investigatory reason to keep Lee in place at LANL and that DOE should feel free to remove him to protect against further disclosures of classified information. In October 1997, Director Freeh delivered the same message to Energy Secretary Federico Pena that he had given to Moler.⁵³ These warnings were not acted on, and Dr. Lee was left in place as were the files he had downloaded to the unclassified system, accessible to any hacker on the Internet.

After the rejection of the FISA warrant request on 12 August 1997, it took the FBI three and a half months to send a memo dated 19 December 1997 to the Albuquerque Field Office listing 15 investigative steps that should be taken to move the investigation forward. The Albuquerque Field Office did not respond directly until 10 November 1998. The 15 investigative steps were principally in response to the concerns raised by OIPR about the previous FISA request. To protect sources and methods, the specific investigative steps in the teletype of 19 December 1997 cannot be disclosed but have been summarized by the FBI as follows:

- Conduct additional interviews:
 - Open preliminary inquiries on other individuals named in the DOE AI who met critical criteria.
 - Develop information on associate's background and interview the associate.
 - Interview coworkers, supervisors, and neighbors.

- Conduct physical surveillance.
- Conduct other investigative techniques:
 - Review information resulting from other investigative methods.
 - Review other investigations for lead purposes.
 - Implement alternative investigative methods.⁵⁴

As best as can be determined at this time, only two of the leads were seriously pursued. Most important, the FBI did not open investigations on the other individuals named in the DOE AI until recently.

The FBI conducted a false-flag operation against Dr. Lee in August 1998, in which an FBI agent posing as a Chinese intelligence officer contacted Lee. The FBI agent provided Dr. Lee with a beeper number and a hotel name. Dr. Lee did not immediately report this contact, but he told his wife who told a friend, who told DOE security. When Dr. Lee was questioned by DOE counterintelligence personnel about the phone call, he was vague and specifically failed to mention the beeper number or the hotel.

These additional steps did yield significant information that was relevant to supporting a determination of probable cause for a renewed FISA warrant, but the information was not used. While the FBI informally told OIPR of Dr. Lee's failure to fully report the August contact, that conversation did not take place until three months after the incident occurred.

The second lead that was pursued related to a potentially sophisticated communications system available to Dr. Lee, the specifics of which cannot be further detailed in this report for security reasons. This information, developed by the new agent in charge of the case and included in the 10 November 1998 FBI Albuquerque request for a new FISA application, would have been very important to OIPR's concerns about whether Dr. Lee was "currently engaged" in espionage, as well as the requirement for the activity to be clandestine.

Despite the development of significant relevant information on the probable cause issue, the FBI never made another formal request for DOJ to approve a new FISA warrant application after the OIPR decision in 1997 not to send the request forward. When such serious national interests were involved in this case, it was simply unacceptable for the FBI to tarry from 12 August 1997 to 19 December 1997 before sending the Albuquerque Field Office a memo. It was equally unacceptable for the Albuquerque field office to take from 19 December 1997 until 10 November 1998 to respond to the guidance from Headquarters, and then for the FBI not to renew the request for a FISA warrant based on the additional evidence.

DOE's Interference in the Investigation

Dr. Lee traveled to Taiwan during the first three weeks of December 1998. The FBI agent who took over the case on 6 November 1998 did not agree with the DOE decision to have Wackenhut⁵⁵ give Dr. Lee a polygraph examination upon his return from Taiwan on 23 December 1998 and has called it "irresponsible." According to FBI protocol, Dr. Lee would have been questioned as part of a post-travel interview. However, the case agents were inexplicably unprepared to conduct such an interview. Ultimately, the polygraph decision was coordinated between DOE and the FBI's National Security Division. It should be noted, however, that the agent's concerns were supported by the report of June 1999 by the President's Foreign Intelligence Advisory Board, which recommended that the Attorney General determine, among other things, "why DOE, rather than the FBI, conducted the first polygraph in this case when the case was an open FBI investigation"⁵⁶

There was no good reason for DOE to polygraph Dr. Lee in late 1998. There was no sudden change in status on the case: the last warning from the FBI about the need to remove Dr. Lee's classified access to protect national security had come some 14 months before, in October 1997. Available Department of Energy documents do not address this question. Other sources, including an FBI

HQ memorandum for Director Freeh, dated 21 December 1998, and a sworn deposition from an FBI agent who worked on the case, indicate that senior DOE officials were concerned about the imminent release of the *Cox Committee Report* and wanted to bring the case to a conclusion.

Even more important than the question of why DOE, rather than FBI, administered this polygraph is the way the results were reported. It should be noted that, as late as March 2000, there still exists considerable disagreement between the FBI and the DOE regarding the sequence and timing of events related to the production of information about the 23 December 1998 polygraph. When given an opportunity to contest the FBI's representation of the facts, DOE's Mr. Ed Curran said they were incorrect but was not prepared with specific contradictory information to offer as evidence. The resolution of these disagreements may ultimately turn on the credibility of the individuals involved in the disagreement and will be the subject of a future subcommittee hearing. According to the record as it now stands, the FBI was told on 23 December that Dr. Lee had passed the polygraph. The agents who were handling the case were given a summary sheet to support this conclusion but were not given access to the actual polygraph charts or the videotape of the interview.

Although DOE's quality-control review process apparently changed the interpretation of the polygraph results—concluding that Dr. Lee should be questioned again on key issues—that information was not immediately provided to the FBI. According to FBI records, the FBI's Albuquerque office did not receive the charts and videotapes from the 23 December polygraph until 22 January 1999. When FBI polygraph experts in early February subsequently analyzed the charts and videotape, they concluded that Dr. Lee had failed relevant questions⁵⁷ or was, at best, inconclusive.⁵⁸ Based on these concerns, the FBI arranged for additional interviews and a new polygraph on 10 February 1999.

The DOE failed to keep the FBI fully informed on the polygraph issue in a timely fashion. Although they were present at the exam, FBI agents did not

receive the polygraph charts until a month later, even though Wackenhut quality-control personnel had assessed the charts on 23 December and again on 28 December. No satisfactory explanation has yet been offered for this delay. It should be noted, however, that according to an FBI memorandum of 26 February 1999, DOE employees were initially instructed not to provide the FBI with the full results of the polygraph, only the summary sheet.

On this state of the record, it appears that DOE did take the position that Dr. Lee passed the 23 December polygraph. As late as 16 March 1999, Energy Secretary William Richardson said on *CNN Crossfire* that DOE “instituted a polygraph on this person, which he first passed.”⁵⁹ Secretary Richardson then described a second polygraph, apparently referring to the FBI-administered polygraph in February, which Dr. Lee failed.

Given the representation by DOE that Dr. Lee passed the polygraph, it is not surprising that the FBI’s investigation of Dr. Lee was thrown off course in late 1998. In contrast with the FBI’s renewed efforts for the FISA warrant—as laid out in the teletype of 10 November 1998 from the Albuquerque office—when told by DOE that Dr. Lee had passed the polygraph, the FBI interviewed him on 17 January 1999,⁶⁰ and in a teletype dated 22 January 1999 to FBI HQ, in effect, concluded that the investigation should not be pursued.

In late January 1999, Dr. Lee began erasing the classified files from the unsecured area of the computer. After the interview on 17 January, Dr. Lee “began a sequence of massive file deletions . . .”⁶¹ He even called the help desk at the Los Alamos computer center to get instructions for deleting files. After he was interviewed and polygraphed again on 10 February within two hours of the time he was told he had failed the exam, he deleted even more files. All told, Dr. Lee deleted files on 20 January and 9, 10, 11, 12, and 17 February. When he called the help desk on 22 January, his question indicated that he did not know that the “delay” function of the computer he was using would keep deleted files in the directory for some period of time. He asked why, when he deleted

files, were the ones in parentheses not going away, and asked how to make them go away immediately. On 16 February, he also asked how to replace an entire file on a tape.⁶²

Thus, the report that Dr. Lee had passed the polygraph of 23 December 1998 gave him precious time to delete and secrete information. The significance of Dr. Lee’s file deletions—and the unreasonable delays in carrying out the investigation that should have detected and prevented them—should not be underestimated. As FBI Agent Robert Messemer has testified, the FBI came very close, “within literally days, of having lost that material.”⁶³ The FBI was almost unable to prove that Dr. Lee downloaded classified files. If the material had been overwritten after it was deleted, “that deletion by Dr. Lee [would] have kept that forever from this investigation.” In this context, the repeated delays and the lack of coordination between the FBI and the Department of Energy—and later between the FBI and the Department of Justice—are much more serious.

10 February 1999 to 8 March 1999

On 10 February 1999, Wen Ho Lee was again given a polygraph examination, this time by the FBI. During this second test, which Lee failed, he was asked: “Have you ever given any of [a particular type of classified computer code related to nuclear weapons testing] to any unauthorized person?” and “Have you ever passed W-88 information to any unauthorized person?”⁶⁴ It should be noted that the 1997 FISA request mentioned that the PRC was using certain computational codes, which were later identified as something to which Lee had unique access.⁶⁵ Moreover, the computer code information had been developed independently of the DOE Administrative Inquiry, which is now being questioned by FBI and DOJ officials.

After this second failed polygraph, there should have been no doubt that Dr. Lee was aware he was a suspect in an espionage investigation, and it is inconceivable that neither the FBI nor DOE personnel took the rudimentary steps of checking

to see if he was engaging in any unusual computer activity. Again, this is not hindsight. The classified information to which Dr. Lee had access, and which he had been asked about in the polygraph, was located on the Los Alamos computer system. The failure of DOE and FBI officials to promptly find out what was happening with Dr. Lee's computer after he was deceptive on the code-related polygraph question is inexplicable. As noted above, this failure afforded Dr. Lee yet another opportunity to erase files from both the unsecured system and the unauthorized tapes he had made.

As should have been expected, Dr. Lee used the time afforded him by the delays to delete the classified information he had placed on the unclassified system. He also approached two other T-Division employees with a request to use their tape drive to delete classified data from two tapes (he no longer had access to the one that had been installed in his X-Division computer since he had been moved from that division in December 1998).

Nearly three weeks after the polygraph failure, the FBI finally asked for and received permission to search Lee's office and his office computer, whereupon they began to discover evidence of his unauthorized and unlawful computer activities. Even so, the FBI did not immediately move to request a search warrant. The three-week delay, from 10 February until the first week of March, is inexplicable.

8 March 1999 to 7 April 1999

Dr. Lee was fired on 8 March 1999. While it is difficult to understand why the FBI did not move more quickly after the February polygraph failure, the subsequent delay—from when Wen Ho Lee was fired on March 8, until a search warrant for his home was finally obtained on April 9—is equally inexplicable. Rather than moving quickly to discover the extent of the potential damage, FBI and DOJ officials continued to wrangle over whether the matter should be handled under FISA or was “way too criminal” for that.⁶⁶ Meanwhile, information that could change the global strategic

balance was left exposed on an unclassified computer system where even an unsophisticated hacker could gain access to it.

It was not until nearly a month after Lee was fired that progress was made on the search warrant issue. Only after a meeting on 7 April 1999, when FBI officials indicated that FBI Director Freeh was “prepared formally to supply the necessary certifications that this search met the requirements of the FISA statute—that is, that it was being sought for purposes of intelligence collection (*e.g.*, to learn about Lee's alleged contacts with Chinese intelligence),”⁶⁷ did the search warrant process begin to move forward.

At this 7 April meeting, OIPR attorneys raised their old concerns about the currency and sufficiency of the evidence against Lee, as well as new concerns about the appearance of improperly using FISA for criminal purposes and the prospect of conducting an unprecedented overt FISA search.⁶⁸ Frustrated that the Criminal Division continued to believe that the FBI's draft affidavit contained an insufficient showing of probable cause to search Lee's residence, FBI officials began working with an Assistant US Attorney in Albuquerque to craft a second affidavit that was presented to a US Magistrate Judge on 9 April 1999 and was executed without incident the following day.⁶⁹

Reopening the W-88 Investigation and the Criminal Case Against Dr. Lee

The decision in September 1999 by the FBI and the DOJ to expand the investigation of suspected Chinese nuclear espionage⁷⁰ is puzzling, primarily because it should have happened long ago. Assistant FBI Director Neil Gallagher's letter of 10 November 1999 on the question of why the investigation is being reopened raises more questions than it answers. He acknowledges that, when discussing the DOE's AI during his 9 June 1999 testimony before the Governmental Affairs Committee,⁷¹ he stated that, he “had full credibility in the report,” had “found nothing in DOE's AI, nor the conclusions drawn from it to be erroneous,” and

stated there is a “compelling case made in the AI to warrant focusing on Los Alamos.”⁷²

As a result of further inquiry, however, Mr. Gallagher now has reason to question the conclusions of the AI. He cites an interview on 20 August 1999 by FBI officials of one of the scientists who participated in the technical portion of the AI, in which the scientist “stated that he had expressed a dissenting opinion with respect to the technical aspects of the AI,” and points out that the statement of this scientist is “in direct conflict with the AI submitted to the FBI because the AI does not reflect any dissension by the ‘DOE Nuclear Weapons Experts.’”⁷³

Although both the FBI and the DOE have repeatedly promised to do so, neither agency has yet provided an answer as to how many scientists were involved in the technical review mentioned in the interview of August 1999 and what the majority opinion of that group really was. Mr. Gallagher explains that “a review has been initiated by the FBI to re-evaluate the scope of the AI,” and that, “the focus of this new initiative is to determine the full universe of both compromised restricted nuclear weapons information and who had access to that information in addition to anyone identified in the original AI.”⁷⁴

The delay by DOJ and the FBI until September 1999 is perplexing since four governmental reports had concluded—with varying degrees of specificity—that the losses of classified information extended beyond W-88 design information and beyond Los Alamos:

- The classified version of the *Cox Committee Report* (January 1999).
- The damage assessment of 21 April 1999 by Mr. Robert Walpole, the National Intelligence Officer for Strategic and Nuclear Programs.⁷⁵
- The unclassified version of the *Cox Committee Report* (May 25, 1999).
- The *Special Report of the President’s Foreign Intelligence Advisory Board* (June 1999).

All of these reports gave FBI and DOJ ample evidence that further investigation was necessary. For example, the *Cox Committee Report* states flatly, “the PRC stole classified information on every currently deployed US inter-continental ballistic missile (ICBM) and submarine-launched ballistic missile (SLBM).”⁷⁶ Tellingly, the Cox Committee notes that, “a Department of Energy investigation of the loss of technical information about the other five US thermonuclear warheads had not begun as of January 3, 1999 . . .” and that, “the FBI had not yet initiated an investigation” as of that date.⁷⁷ Thus, the failure to reopen the investigation into the loss of W-88 design information much sooner, or to even initiate an investigation of the other losses, simply continued that pattern of errors.

The subcommittee’s investigation thus far has identified several areas where reform is necessary and identified appropriate solutions. These solutions have been incorporated in the “Counter-Intelligence Reform Act of 2000,” which is summarized below:

1. This bill amends the Foreign Intelligence Surveillance Act by providing that, upon the personal request of the Director of the FBI, the Secretary of State, the Secretary of Defense, or the Director of Central Intelligence, the Attorney General shall personally review a FISA application. The failure to forward the FISA request to the court in 1997 represents a critical failure in this case. When the “global strategic balance” is an issue, the Attorney General should not delegate the review to subordinates with no experience in FISA matters, as happened in this instance. Because this provision is triggered only by a personal request from the Director of the FBI or one of the other few Cabinet officials authorized to request FISA warrants, it will not impose upon the duties of the Attorney General except in truly exceptional cases where such imposition is clearly warranted.
2. If the Attorney General decides not to forward the application for a warrant to the

court, that decision must be communicated in writing to the requesting official with specific recommendations on what additional investigation should be undertaken to establish the requisite probable cause. A decision to reject a FISA application should come only after careful analysis of the specifics. Should the Attorney General still decline to go forward with a request after such analysis, the requesting agency should have the benefit of that analysis, as well as a plan to remedy any deficiencies. By definition, this section will apply only in cases where the Director of the FBI or another senior Cabinet official has made a personal appeal to the Attorney General. By communicating the reasons for the rejection in writing, along with recommendations for improvements, the Attorney General can facilitate the proper functioning of the FISA process to ensure that the national security is not put at risk due to misunderstandings about the showing of probable cause in a case.

3. The requesting official must personally supervise the implementation of the Attorney General's recommendations. The FBI's delay of three and a half months after the decision in August 1997 regarding the FISA application and the delay from 19 December 1997 until 10 November 1998 for a response by the Albuquerque office was unacceptable in the context of the national security information at risk. In cases of such great importance, the personal knowledge and supervision by top officials is appropriate and necessary.
4. This bill addresses the issue of whether an individual is "presently engaged" in the particular activity in order not to preclude conduct in the past from serving as the basis for a warrant—even if a substantial period of time has elapsed—recognizing that espionage or related activities usually span a considerable period of time, causing the legislature to omit any statute of limitations for such crimes. Where directly relevant conduct has occurred in the past, it should not be excluded if it reasonably can be interpreted as indicating that

an individual is involved in espionage. OIPR's focus on the contention that the W-88 information had been lost some ten years earlier was clearly misplaced. The loss of our national security information is so important that it must be investigated, even if discovered somewhat after the fact. Keeping in mind that FISA surveillance is primarily for intelligence rather than for criminal purposes, such events should not be unnecessarily excluded from consideration.

5. Finally, this bill improves the coordination of counterintelligence activities by requiring that:
 - a. If the FBI requests a FISA warrant on an individual with whom it or any law enforcement or intelligence agency has a relationship, that fact must be disclosed to OIPR as part of the FISA request.
 - b. When the FBI desires to leave an individual in place for investigative reasons, that decision must be communicated in writing to the head of the affected agency, along with a plan to minimize the potential for harm to the national security, which shall take precedence over investigative concerns. The agency head must, likewise, respond in writing, and any disagreements over the proper course of action will be referred to the National Counterintelligence Policy Board.
 - c. When the FBI opens a counterintelligence investigation on a subject, it must coordinate with other intelligence and law enforcement agencies to identify any relationship between the subject and those entities.

I urge prompt consideration of these proposals.

Endnotes

¹ Stephen Younger, "Transcript of Proceedings, Detention Hearing in the case of United States vs. Wen Ho Lee," 13 December 1999: 38 (hereafter referred to as Transcript of Proceedings).

² Transcript of Proceedings, 38.

³ Transcript of Proceedings, Motion Hearing, 27 December 1999: 4. (hereafter referred to as Motion Hearing).

⁴ This information was drawn from Dr. Lee's Web site at <http://wenholee.org/whois.htm>.

⁵ United States of America, "Response to Defendant Wen Ho Lee's Motion to Revoke Judge's Order of Detention," 23 December 1999: 10. See also, United States Senate, Selection Committee on the Judiciary, Redacted Transcript of Closed Hearing with Attorney General Janet Reno Regarding the FISA Process in the Wen Ho Lee Case, 8 June 1999: 14-16.

⁶ Ibid. 10. See also, United States Senate, Select Committee on the Judiciary, Redacted Transcript of Closed Hearing with Attorney General Janet Reno Regarding the FISA Process in the Wen Ho Lee Case, 8 June 1999: 15 (hereafter referred to as Redacted Transcript).

⁷ Redacted Transcript, 15.

⁸ Redacted Transcript, 15.

⁹ "Response to Defendant Wen Ho Lee's Motion to Revoke Judge's Order of Detention," 23 December 1999: 13, footnote 4.

¹⁰ Ian Hoffman, "Agent: Lee Admitted Lying," *Albuquerque Journal*, 18 January 2000, online edition.

¹¹ Redacted Transcript, 16.

¹² Redacted Transcript, 16-17; Senators Thompson and Lieberman's statement, 6, 16.

¹³ James Risen and David Johnston, "U.S. Will Broaden Investigation of China Nuclear Secrets Case," *New York Times*, 23 September 1999, online edition. Notes. 55.

¹⁴ Senators Thompson and Lieberman's statement, 6, footnote 14.

¹⁵ Redacted Transcript, 108-109.

¹⁶ Redacted Transcript, 109.

¹⁷ Redacted Transcript, 109.

¹⁸ Ian Hoffman, "Lawyer: Lee's Intent in Question," *Albuquerque Journal*, 5 January 2000 at <http://wenholee.org/ABQJournal010500.htm>.

¹⁹ For a discussion of this issue, see Motion Hearing, 147-157.

²⁰ Motion Hearing, 152-153.

²¹ United States of America, "Response to Defendant Wen Ho Lee's Motion to Revoke Judge's Order of

Detention," 23 December 1999.

²² William Broad, "Spies Versus Sweat: The Debate Over China's Nuclear Advance," *New York Times*, 7 September 1999, online edition.

²³ Vernon Loeb and Walter Pincus, "China Prefers the Sand to the Moles," *Washington Post*, 12 December 1999, A02.

²⁴ United States House of Representatives, *Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China*, 25 May 1999: Volume 1, 83-84 (hereafter referred to as *Cox Report*). A "walk-in" is an individual who voluntarily offers to conduct espionage.

²⁵ President's Foreign Intelligence Advisory Board, *Science at its Best; Security at its Worst*, June 1999, 30-31 (hereafter referred to as PFIAB).

²⁶ Senators Thompson and Lieberman's statement, 6-7.

²⁷ X-Division Open Lan Rules of Use, executed by Dr. Wen Ho Lee on April 19, 1995.

²⁸ Senators Thompson and Lieberman's statement, 9.

²⁹ "Richardson Announces Results of Inquiries Related to Espionage Investigation," Department of Energy News Release, 12 August 1999.

³⁰ Senators Thompson and Lieberman's statement, 9.

³¹ This list has been extracted from the 5 August 1999, Statement by Senate Governmental Affairs Committee Chairman Fred Thompson and Ranking Minority Member Joseph Lieberman, *Department of Energy, FBI, and Department of Justice Handling of Espionage Investigation into the Compromise of Design Information on the W-88 Warhead*, 14-17.

³² Hydrodynamics is a science that is relevant to the development of nuclear weapons design.

³³ Redacted Transcript, 35 and 88.

³⁴ Redacted Transcript, 118-119.

³⁵ Redacted Transcript, 52. In a 6 March 2000 letter from Assistant Attorney General Robert Rabin to Senator Hatch, the Department of Justice takes issue with this statement and quotes Senator Kyl's testimony on the subject, "So it would be your view that (the language quoted in the draft report) is a summary that probably overstates the Justice Department's requirements for the FBI? The Attorney General responded, "That is correct." Transcript of 8 June 1999 at 49." (sic) For the actual exchange, see page 53 of the 8 June 1999 transcript.

³⁶ Redacted Transcript, 52.

³⁷ Redacted Transcript, 52.

³⁸ Unclassified excerpt of Mr. Seikaly's testimony before the Senate Select Committee on Intelligence, May 1999.

³⁹ Redacted Transcript, 49.

⁴⁰ Redacted Transcript, 49.

⁴¹ Redacted Transcript, 24-25.

⁴² Redacted Transcript, 39.

⁴³ Redacted Transcript, 39..57.

⁴⁴ Redacted Transcript, 40.

⁴⁵ Redacted Transcript, 36.

⁴⁶ Redacted Transcript, 56.

⁴⁷ Redacted Transcript, 117.

⁴⁸ Redacted Transcript, 117.

⁴⁹ Motion Hearing, 85. See also Pete Carey, "Los Alamos Suspect May Have Been Doing His Job: Rerouting Files Common at Lab," *Florida Times-Union*, 20 June 1999, G-8.

⁵⁰ "With Intent to Injure the U.S.," *Washington Times* editorial, 14 December 1999, A16.

⁵¹ United States of America, "Response to Defendant Wen Ho Lee's Motion to Revoke Judge Svet's Order of Detention," December 23, 1999, 3-4.

⁵² Ian Hoffman.

⁵³ Senators Thompson and Lieberman's statement, 23-24.

⁵⁴ Unclassified summary of the 19 December 1997, FBIHQ teletype to Albuquerque, provided by FBI Office of Public and Congressional Affairs, 3 December 1999.

⁵⁵ Wackenhut is a private company that has a contract with DOE to perform security-related polygraphs.

⁵⁶ PFIAB, 34.

⁵⁷ See FBI Headquarters internal memo dated 2 February 1999 and/or 6 February 1999 on the same subject.

⁵⁸ United States Senate, Committee on Governmental Affairs, testimony from 9 June 1999 closed hearing: 145.

⁵⁹ The information regarding Secretary Richardson's public statements on the polygraph question can be found in footnote 108 of the 5 August 1999, special statement of the Senate Governmental Affairs Committee. 58.

⁶⁰ Transcript of Proceeding, Detention Hearing, in the case of U.S. v. Wen Ho Lee, December 13, 1999, before the Honorable Don J. Svet in the U.S. District Court for the District of New Mexico: 118.

⁶¹ Transcript of Proceeding, 118.

⁶² For a detailed discussion of Dr. Lee's deletions and his call to the computer help line, see "Transcript of Proceedings, Motion Hearing, December 27, 1999," *United States of America vs. Wen Ho Lee*, pages 132-138.

⁶³ Transcript of Proceedings, 146.

⁶⁴ Senators Thompson and Lieberman's Statement, 26.

⁶⁵ For a detailed discussion of the computer code issue, see the transcript of Attorney General Reno's testimony

before the Senate Judiciary Committee on 8 June 1999, 108-109 (as numbered in the lower right-hand corner).

⁶⁶ For a discussion of the debate between FBI and DOE after Lee's computer was searched, see Senators Thompson and Lieberman's statement, 27-29.

⁶⁷ Senators Thompson and Lieberman's statement, 28.

⁶⁸ Senators Thompson and Lieberman's statement, 28-29.

⁶⁹ Senators Thompson and Lieberman's statement, 27-28. In a 6 March 2000 letter to Senator Hatch, Assistant Attorney General Robert Rabin expressed the views of the Department of Justice on the subpoena issue, " . . . the Department disagrees with the draft's characterization of the role the Criminal Division played in obtaining a search warrant for Mr. Lee's residence. The Criminal Division in Washington and the US Attorney's Office in Albuquerque worked together throughout the process of obtaining a search warrant for Wen Ho Lee's home. After discussing the issue together, both offices agreed that the first draft search warrant affidavit needed additional facts to establish probable cause. That conclusion was communicated in a joint conference call of both Offices with the FBI. The revised affidavit submitted by the FBI was reviewed and approved by both Offices working together, and was then presented to the US Magistrate Judge on 9 April 1999.

⁷⁰ For example, see the 28 September 1999 press release from the FBI National Press Office, which states that Special Agent in Charge Steve Dillard "has been appointed as Inspector in Charge of a task force composed of FBI Special Agents and analysts that will investigate the possible theft or compromise of classified information from United States nuclear laboratories . . ." The full text of the press release is available at <http://www.fbi.gov/pressrm/pressrel/dillard.htm>.

⁷¹ He made similar representations in other briefings provided to Senate staff.

⁷² Gallagher, letter of 10 November 1999, 1.

⁷³ Gallagher, letter of 10 November 1999, 2.

⁷⁴ Gallagher, letter of 10 November 1999, 2-3.

⁷⁵ See "DCI Statement on Damage Assessment," at http://www.cia.gov/cia/public_affairs/press_release/ps042199.html, and the "Key Findings" at http://www.cia.gov/cia/public_affairs/press_release/0421kf.html.

⁷⁶ *Cox Committee Report*, Vol. 1, 68.

⁷⁷ *Cox Committee Report*, Vol. 1, 83-84

David Tzu Wvi Yang and Eugene You Tsai Hsu

On 30 August 2001, US Customs arrested David Tzu Wvi Yang and Eugene You Tsai Hsu for attempting to export military encryption technology to China in violation of the Arms Control Export Act.

According to an affidavit filed in federal court, Hsu—of Blue Springs, Missouri—and Yang—of Temple City, California—were attempting to export to China encryption devices used to secure and safeguard classified communications. Hsu was arrested at his home in Blue Springs, Missouri. Yang was arrested at his place of business in Compton, California.

The KIV-7HS encryption unit/technology is designed for government use only and cannot be legally exported from the United States without first obtaining an export license from the State Department. China, however, is prohibited from acquiring KIV-7HS unit/technology from the United States.

In May 2001, Hsu contacted Mykotronx, Inc., a private company located in Columbia, Maryland, to inquire about the cost of the KIV-7HS unit/technology. A security officer at Mykotronx subsequently contacted US Customs agents in Baltimore to alert them to Hsu's interest in obtaining the technology. US Customs agents instructed Mykotronx to inform Hsu that all future inquiries relative to the KIV-7HS units would be handled through an intermediary import/export entity located in Maryland.

During the period 2 May to 18 August 2001, an undercover Customs agent, posing as the intermediary, engaged in a series of telephone conversations and faxed correspondence with Hsu, Charlson Ho, and David Yang. The telephone conversations and correspondence revealed that Ho, affiliated with Wei Soon Loong Private, LTD., a Singapore-based company, was the buyer of the KIV-7HS units.

Ho disclosed to the Customs undercover agent that his freight forwarder, David Yang, would handle the export of the KIV-7HS units through his business in Compton, California—Dyna Freight. A check of Immigration and Naturalization Service (INS) records indicated that Yang was born in Taiwan and is a permanent resident alien of the United States.

The undercover Customs agent advised Hsu that the KIV-7HS units are Munitions List items and would require a license for export. Hsu asked if the undercover agent could obtain the license. After being told by the undercover agent that no license would be approved for export to China and that export to China would be a violation of the Arms Control Export Act, Hsu continued to show interest. A check of INS records confirmed that Hsu is a naturalized US citizen.

On 24 August 2001, Yang confirmed to the Customs undercover agent that the KIV-7HS units would be shipped from Los Angeles through Taipei to Singapore, where Ho would then forward the units to China.

PUBLIC ANNOUNCEMENT**U.S. DEPARTMENT OF STATE
Office of the Spokesman****CHINA****April 19, 2001**

The Ministry of State Security (MSS) of the People's Republic of China has recently taken into custody several American citizens and U.S. permanent residents of Chinese origin. Of these, at least two Americans are now being detained by the Chinese authorities under suspicion of espionage or damaging China's national security, even though the Chinese Government has not offered any evidence to substantiate these allegations. Others have been questioned for up to four days and then released.

The Department of State cautions Americans, especially Americans originally from China, that there may be a risk of being detained upon returning to China, if they have at any time engaged in activities or published writings critical of Chinese government policies. In some cases, travel to Taiwan or involvement with Taiwan media organizations has apparently also been regarded as the equivalent of espionage by MSS. Therefore, persons with a history of such activities or writings should carefully evaluate this information in deciding whether to travel to China.

It should be noted as well that the Americans recently detained by MSS had previously visited China without incident, but were nonetheless detained during their most recent visits. At least two of the Americans were identified by MSS as persons of interest, even though they had changed their names in the U.S. upon naturalization or marriage.

CHAPTER 2

INTRODUCTION

In the early 1990s, the new Russian counterintelligence service embarked on a mission to reclaim the former KGB's internal security power, which had been diminished with the fall of the Soviet Union in 1991. A spate of press articles in early 1996 by spokesmen for the Federal Security Service (FSB) boasted the service's role in protecting the state from foreign subversion. FSB officers noted that the service has the responsibility to monitor foreign astronauts at "Star City" and to prevent the emigration of Russian scientists. The FSB has also bragged about the arrest of Israeli, Turkish, and North Korean spies and the expulsion of a British businessman and an Israeli diplomat. The government moves against ecologists further revealed a resurgence of FSB internal power.

Although there continues to be mutually beneficial cooperation between Washington and Moscow, relations between the two countries deteriorated after the election of Vladimir Putin to the Russian presidency on 26 March 2000. Both countries accuse one another of increased espionage activity. However, in light of the terrorist attack on the World Trade Center in New York and the Pentagon in Washington, both sides are cooperating to bring the terrorist organization run by Usama bin Laden to justice.

Internally, the FSB has increased its visibility. One reason for this heightened FSB profile is the personnel changes made by Putin who brought in people he worked with in St. Petersburg or in the security apparatus. Putin stated that he was seeking a professional government that could include members of various political factions. Some observers, however, raised civil rights concerns about a government that was heavily staffed by personnel with long careers in the Soviet-era security apparatus. Putin promoted Sergey Ivanov, Secretary of the Security Council, who is an ex-KGB officer and close friend and Nikolay Patrushev, FSB Director, who knew Putin

in the Leningrad KGB.¹ Putin also quietly replaced fourteen presidential representatives in the regions with former security officers.

FSB director Patrushev said that, in 1999, his service stopped the activities of 65 foreign individual officers and prevented 30 Russian citizens from passing secrets to foreign intelligence services. In 1998, the FSB foiled the activities of 11 intelligence officers and caught 19 Russian citizens attempting to sell classified information to foreign secret services. And in 1996, then-FSB chief Nikolai Kovalyov said the FSB had exposed 400 employees of foreign intelligence services and 39 Russians working for them during the period 1994-96.

The Sutyagin case follows the sentencing in December 2000 of retired US Navy officer Edmund Pope to 20 years for spying. Pope, who was arrested and charged with espionage, was the first American to be sentenced for espionage in Russia for 40 years, although he was quickly pardoned by Putin and returned to the United States. Following the Pope case, the FSB arrested American John Tobin on drug charges but continued to suspect he was an intelligence operative. They also told an American teacher, Elizabeth Swift, to leave Russia.

In the United States, two former Soviet agents were finally caught. On 13 October 1998, the FBI arrested retired US Army intelligence analyst David Sheldon Boone charging him with selling secrets to Moscow. George Trofimoff, a retired Army colonel, was arrested on 13 June 2000 and accused of spying for the Soviet Union in a 25-year-long Cold War conspiracy. Both men were later convicted of espionage.

On 8 December 1999, the FBI detained Russian intelligence officer Stanislav Gusev as he was recording transmissions from a bug implanted in a

Department of State conference room. Gusev was declared persona non grata and required to leave the United States.

In February 2001, the FBI arrested Robert Hanssen, one of its most senior counterintelligence officers, on charges of spying for Russia between 1985 and 2001. On 21 March, the United States expelled four Russian diplomats for alleged espionage activity in connection with the Hanssen case. At the same time, 46 other Russian diplomats believed to be intelligence officers were ordered to leave the country, a move reportedly aimed at reducing the heightened level of Russian espionage activity in the United States. This was the largest such expulsion since President Ronald Reagan ordered the expulsion of 80 diplomats in 1986. On 22 March, Russia retaliated, expelling four US diplomats and announcing that 46 more were ordered to leave by July.²

In January 2001, there was reporting that the Russian Government was considering reorganizing its intelligence apparatus. Ivanov, secretary of the Russian advisory Security Council, was quoted by Russian press agencies as saying that strengthening the links between the services was one of the priority issues for the next six months. The likely services involved would be the FSB, the Border Guards, and FAPSI, which is responsible for intercepting communications. In November 2000, the government had proposed draft legislation in the Russian parliament to reunify the intelligence services, but it created such concern by liberal critics about recreating a KGB-type organization that the measure did not pass.³

Konstantin Preobrazhensky, a security analyst and former KGB officer, who is now a strong critic of the services, said he doubted that the intelligence

services could be reunited as a single entity. He said that each service—including the SVR—had its own ministerial-level chief who would not be in favor of relinquishing power or serving under a single head.

Endnotes

¹ Richard Staar, Perspective, March-April 2000; Federal News Service, 29 March 2000.

² Stuart D. Goldman, *Russia*, Congressional Research Service, The Library of Congress, 26 March 2001.

³ Andrew Jack, "Shake-up could revive KGB," *Financial Times*, 8 January 2001.

Theodore Alvin Hall

On 1 November 1999, Theodore Alvin Hall died of cancer in Cambridge, England, at the age of 74. As a 19-year-old Harvard physicist, he helped develop the atomic bomb at Los Alamos, New Mexico, during World War II and also passed the vital secrets of his work to the Soviet Union. A Soviet cable declassified by the National Security Agency in 1995 identified Hall and his Harvard roommate, Saville Sax, as Soviet informants.

The FBI had questioned Hall and Sax in 1951, but did not press charges for lack of evidence. The vital secrets of his work involved the “implosion principle,” developed at Los Alamos as a way to ignite an atomic bomb. At the time the cable was published, Hall was at the end of a distinguished career at Cambridge University, where he had been a pioneer in developing biological X-ray microanalysis.

Hall was quoted in 1997 as saying that, in 1944, he was concerned about the dangers of an American monopoly of atomic weapons if there was a postwar depression, and he contemplated meeting with the Soviets to inform them of the existence of the atomic bomb project. He reportedly passed a description of the implosion principle to Sax, who took it to their Soviet control officer in New York City. Sax died in 1980. Neither Sax nor Hall was ever charged with espionage.

State Department Security Breaches

Significant security breaches occurred at the Department of State, which this series of incidents reveals serious deficiencies in security awareness, practice, and culture at the Department.

In February 1998, an unidentified man, wearing a tweed jacket, entered the Secretary of State’s seventh floor office suite and removed classified documents, including documents classified as Sensitive Compartmented Information (SCI). The man in this “tweed jacket incident” has never been identified, and the documents have never been recovered. In addition, poor procedures for handling classified information resulted in the Department’s inability to reconstruct which documents were taken. Without such information, a full and complete damage assessment was not possible.

In January 2000, a laptop computer containing highly sensitive classified intelligence materials, including SCI material relating to weapons proliferation, was discovered to be missing from the State Department Bureau of Intelligence and Research (INR) and is presumed stolen. Despite an obligation under the National Security Act of 1947 to keep the intelligence committees “fully and currently informed of all intelligence activities,” including “significant intelligence failures,” the Committee was not informed of the loss of this laptop computer until after *The Washington Post* reported the story in April 2000.

Following the “tweed jacket” affair, the SSCI, in the Annex to the Intelligence Authorization Act for Fiscal Year 1999, directed the State Department Inspector General (IG) to review and report on State Department policy and procedures for handling classified information within the State Department Headquarters facility. The September 1999 IG report, entitled “Protecting Classified Documents at State Department Headquarters,” found that “[t]he Department [of State] is substantially not in compliance with the DCIDs [Director of Central Intelligence Directives] that govern the handling of SCI.”

In response to the IG report in the Annex to the Intelligence Authorization Act for Fiscal Year 2000, the Congressional intelligence committees required (1) a report from the DCI evaluating the State Department's compliance with all DCIDs related to the protection of Sensitive Compartmented Information, (2) a State Department report on specific plans for enhancing the security of classified information within the State Department, and (3) full implementation, as appropriate, of the recommendations found within the IG's report.

The February 2000 DCI report noted that an independent review by the CIA and the Community Management Staff confirmed that the State Department was not in compliance with applicable DCID requirements. The report concluded that certain additional steps were required to "improve security practices in Department offices where SCI is handled and discussed, as well as to strengthen SCI document control and accountability." In its report the State Department identified a number of actions or proposed actions it intended to take in response to the IG report.

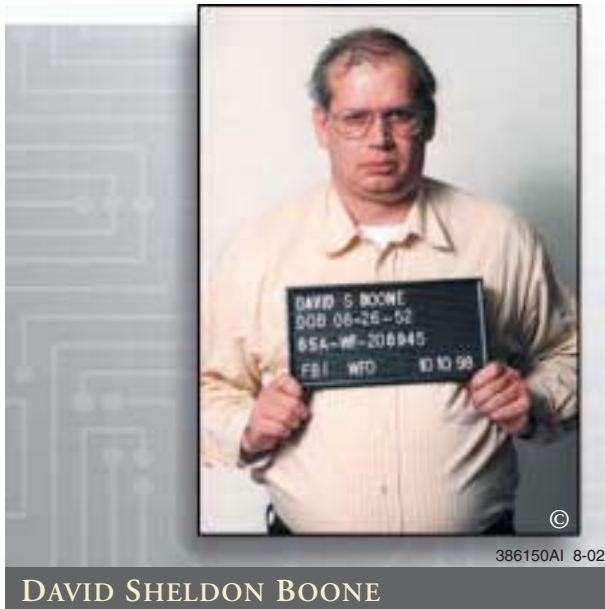
In the wake of the missing laptop computer incident, Secretary of State Madeline Albright declared her intention to transfer positions and responsibility for ensuring the proper security and handling of SCI material from INR to the Bureau of Diplomatic Security (DS). At that time, the Committee expressed its concerns regarding this transfer, including the need to ensure continued DCI oversight over SCI material at the State Department and the requirement that this function should be funded through the National Foreign Intelligence Program (NFIP) budget.

Such oversight and budgetary authority is critical to ensure effective implementation of measures to protect intelligence information at the State Department. In the fall of 2000, the DCI's Community Management Staff and the Department of State agreed to measures designed to ensure continued DCI oversight of the protection of SCI material and continued funding for this function within the NFIP.

In the Intelligence Authorization Act for Fiscal Year 2001, the Committee required the Director of Central Intelligence, in the wake of high-profile security breaches at the State Department, to certify State Department compliance with applicable standards regarding the handling, retention, or storage of SCI material. Elements of the State Department that the DCI does not certify as in compliance, or that do not receive a DCI waiver, would not retain or store SCI information until they are certified as compliant.

In addition, the Committee, in the report accompanying the Intelligence Authorization Act for Fiscal Year 2001, directed the State Department Inspector General to conduct annual reviews of State Department policies and procedures for protecting classified information at the Department for the next five years to determine progress in this area. The Committee took numerous steps to improve the security situation at the State Department and continued to focus this oversight in the future.

David Sheldon Boone



David Sheldon Boone was born on 26 August 1952 in Flint, Michigan. In October 1970, four months after graduating from Mayfield High School in Las Cruces, New Mexico, Boone enlisted in the US Army. He received training in cryptographic analysis and took two Russian language-training courses at the Defense Language Institute. Throughout his military career he served in US Army-related Signals Intelligence (SIGINT) activities. Boone served at the US Army Field Station (USAFS) in Augsburg, Germany, from August 1974 to December 1976, and again from July 1979 to May 1985. After 18 years of service and nearing completion of a three-year assignment to the National Security Agency (NSA) at Ft. Meade, Maryland—from June 1985 until October 1988 where he worked as a senior cryptologic traffic analyst—the US Army selected Boone for a third assignment to USAFS in Augsburg.

At this time, his marriage to his first wife was collapsing, and the couple was having financial problems. In February 1988, Boone took a signature loan for \$2,000 but this did not solve their problems. On 19 October 1988, Boone and his wife entered into a voluntary separation agreement. The agreement provided that Boone's entire US Army pay would go to his wife who would then give

him \$250 monthly—Boone had no other known legitimate sources of significant income. Boone's wife also received custody of both their children.

Boone decided to go unaccompanied to Augsburg for a two-year tour. He stated that neither he nor his wife could manage money. He considered armed robbery as a solution to their money problems and even purchased a shotgun for that purpose, but reconsidered his options. He applied for, but was eventually denied, authorization to leave his family in military family housing on Ft. Meade. Before leaving for Augsburg, he took an advance of three months' pay.

At NSA, Boone was assigned to a unit that analyzed and produced reports on Soviet Fire Support Operations. He also had access to sensitive information about the capabilities and movements of Soviet forces and about Soviet tactical nuclear weapons. Boone's last performance evaluation while assigned to NSA, which he signed on 21 October 1988, rated his overall performance as "fair" and his promotion potential as "marginal." The evaluation noted Boone had a "lack of self-motivation," and that he "lacks attention to detail and tenacity in areas outside of his technical specialty" and "fails to lead by example."

In the wake of the Army's denial to allow his family to remain at Ft. Meade, Boone decided to sell classified information to the Soviet Union. Sometime in September 1988, Boone telephoned the Soviet Embassy on 16th Street NW, Washington DC and requested their hours of operation. A few days after the phone call, Boone drove on his motorcycle to the vicinity of the Embassy and then approached and entered the Embassy grounds on foot. He asked the receptionist to see an attaché.

Boone gave his Ft. Meade and Army photo identification badges to an Embassy employee and, after waiting for some time, was interviewed by three or four Soviets. Boone offered to sell classified information and gave them a classified document that he had written on decrypted NSA intercept information—Boone said that he

first approached the Soviets because, “I needed money. Plus, well, plus I was extremely angry.” He explained his access, his need for money and his pending assignment to Germany. He was given instructions for a follow-on meeting at the Soviet residential complex, \$300, and a disguise consisting of a wig and moustache to use when he returned for the next meeting. After five or six hours in the Embassy, the Soviets put him in an enclosed van and dropped him off some blocks away from the Embassy.

A few weeks later, Boone, following his contact instructions, rode his motorcycle to approximately six to seven blocks away from the Soviet building complex in a residential area of northwest Washington, DC. After parking his motorcycle and wearing his wig and moustache, he walked to the complex and entered it. Boone was led through underground corridors and tunnels and into a room.

The Soviets interviewed Boone for hours during which he provided additional NSA documents that he had selected to demonstrate his access to such information. Boone later stated that to get documents through security and out of the NSA building at Ft. Meade, he would fold up to 15-20 pages of documents and conceal them under the half-liner of his Army windbreaker. The Soviets also debriefed him on NSA’s organization and gave him \$1,500. At the end of the session, the Soviets gave him recontact instructions for Germany. Again the Soviets used the enclosed van to remove him from the complex and returned him to the vicinity of his motorcycle.

In October 1988, Boone reported to his new duty station at Augsburg. He was assigned as the senior enlistee in an Army Technical Control and Analysis Element (TCAE) unit. According to Army publications, the TCAE is responsible for assisting in the technical management and tasking of military SIGINT and Electronic Warfare (EW) systems. TCAE personnel also analyze and report signal intercepts and maintain an extensive technical database to support SIGINT agencies. The TCAE unit at USAFS Augsburg was located within a limited-access Sensitive Compartmented

Information Facility (SCIF). Boone’s duties brought him in regular contact with highly classified and extremely sensitive national defense information.

Shortly after arriving in Germany, Boone met a female German citizen, and in March 1989, he began living with her at her home in Augsburg. Boone disclosed this relationship to Defense Investigate Services (DIS—now Defense Security Service or [DSS])—investigators in June 1990 during his security clearance background investigation.

In June 1990, one of Boone’s supervisors informed DIS investigators that Boone was severely in debt and owed money to creditors, and that Boone’s estranged wife had written to Boone’s commander, claiming Boone was wrongfully retaining from his pay funds that were due to her. Boone acknowledged to the DIS investigators that he owed creditors and told them he had deliberately allowed the debts to accumulate to cause his military pay to be garnished and thus to deprive his wife of the money.

That same month, Boone’s access to classified information was suspended because of his lack of personal and professional responsibility. Boone was reassigned to serve as Sergeant of the guard in a US military hospital at Augsburg, where he remained until his retirement on 1 June 1991.

After retiring from the US Army, Boone continued to reside in Germany. Beginning in September 1991, Boone was employed as a sales engineer, a product support employee, and a support account manager for three successive German computer companies. His divorce from his first wife was final in December 1991, and in 1994, he married the German woman with whom he had lived since 1989.

In November 1988, he met a KGB/SVRR¹ officer whom he came to know as “Igor.” During their first meeting, Boone gave Igor classified documents, and Igor gave Boone \$4,000 and a communications plan that included an emergency meeting site and signal sites.

Boone stated that between late 1988 and the time he retired from the US Army in 1991, he met with Igor approximately four times a year at various locations along the Rhine River. At each meeting, Boone gave Igor classified documents he had obtained since the previous meeting. Igor gave Boone money for the documents Boone had previously passed and they would schedule their next meeting. Boone said that he received \$5,000 to \$7,000 at each meeting, he once received a \$5,000 bonus, and that these payments amounted to \$20,000 to \$22,000 a year, for a total of more than \$60,000 for the period he worked for the KGB/SVRR.

Boone did not deposit the money in a bank, explaining, “It’s called a paper trail. Don’t leave something for anyone to track. It’s called, it’s called, uh, paranoia.” Boone said he used the cash for normal living expenses. He explained that his separation agreement required him to give his entire pay check to his estranged wife who was to supposed to then give Boone \$500 a month for living expenses—the actual figure was \$250 a month but Boone exaggerated the amount during his retelling of the story. His wife never actually sent him any money.

Boone said on one occasion that he left documents in a “drop,” following instructions Igor gave him. Boone described the drop procedure as follows:

I know from my training and experience that a “drop” or “dead drop” is a prearranged location where a foreign agent and intelligence officer may use impersonal, clandestine means of communication to exchange tangible objections. For example, an agent may pass classified documents to his handling officer by placing them in a trash bag and secreting the bag in a log or pipe; later, the handling officer can retrieve the bag without having had personal contact with the agent. Such a technique can reduce the chance that illegal clandestine activity will be detected.

Boone said that during the three years he worked for the KGB/SVRR he chose classified US

Government documents to give to the KGB/SVRR based on three factors:

- Their value to the KGB/SVRR.
- The amount of detailed information they contained.
- The variety of information they represented.

Boone said that Igor would task him for documents he knew Boone had access to or for documents that were referenced in documents the KGB/SVRR had previously obtained. On one occasion, Igor told Boone that the KGB/SVRR had access to the United States Signals Directive (USSID) entitled Zero, which was an index of all other USSIDs, and from this index, Igor asked Boone to obtain specific USSIDs. USSIDs are classified NSA publications for use in providing SIGINT support to the US military.

Boone gave Igor a photocopy of a NSA document entitled “United States Signals Intelligence Directive (USSID) 514, dated 6 May 1988. Boone said that this USSID was unusual because it was one of the few USSIDs to be classified Top Secret rather than Secret. Boone added that USSID 514 was not widely disseminated but that one copy had been at USAFS Augsburg. Boone said he particularly recalled this document because of its “frightening” topic, which he described as “tasking the targeting of US nuclear weapons against Soviet targets.” Boone provided USSID 514 to the KGB/SVRR because it would furnish the Soviets with information regarding US intentions concerning the potential use of nuclear weapons.

The FBI/US Army Intelligence and Security Command (INSCOM) investigation determined that one copy of USSID 514, dated 6 May 1988, was distributed to USAFS Augsburg. Each page of USSID 514 is marked as classified Top Secret and Not Releasable to Foreign Nationals.

In 1989, he gave Igor an original manual, which Boone said was entitled Joint Tactical Exploitation and was probably produced in 1988. Boone explained that although this document was strictly controlled, Boone had access to two numbered originals at USAFS Augsburg and believed one

would not be missed. Boone said the document was classified Top Secret UMBRA, and described the document as 300 to 400 three-holed-punched pages long.

Boone told Igor that he thought this document was “especially valuable” and asked Igor for an increased payment for it. At the next meeting, Igor gave him a \$5,000 bonus. Boone said that, based upon his having provided this document, a reserve fund was set up for him in a Soviet bank, where additional funds were deposited.

The FBI/INSCOM investigation ascertained that in 1988 a limited quantity of a manual entitled Joint-Service Tactical Exploitation of National Systems (J-TENS) had been distributed to military facilities, including two numbered originals to USAFS Augsburg. The J-TENS consists of approximately 300 double-sided pages and is three-hole punched. Each page is marked Top Secret UMBRA, No Foreign Dissemination, and bears other SCI access-restriction markings. The J-TENS is the handbook of US reconnaissance programs and collection systems. It is for use by US military units in obtaining critical time-sensitive information to support tactical military operations. The J-TENS contains the statement: “Disclosure of this information to unauthorized persons would gravely damage the national security of the United States.”

Boone said that when he lost his access to classified information and was arranging to retire, his cooperation with the KGB/SVRR ended. At that time, Boone informed Igor that “I would be willing to help,” although Boone did not specify any particular things that he could do.

In 1994, the FBI began an investigation of an Unknown Subject (UNSUB) espionage allegation. By 1997, the FBI, US Army, and NSA had identified Boone as the primary suspect in the case. Prior to the initial contact between an FBI operational asset and Boone, the three agencies conducted a detailed investigation into Boone’s alleged espionage.

On 5 September 1998, the FBI asset had a telephone conversation with Boone. The asset indicated to Boone that he (the asset) was associated with the KGB/SVRR and wanted to meet with Boone to discuss some proposals that Boone had previously made, to discuss the status of Boone’s reserve account, and to get Boone’s expert opinion on another matter. Boone replied, “Where and when?” The asset suggested a meeting in London, England, the following weekend, and Boone agreed to do so. The asset instructed Boone to check into a hotel in London on 11 September 1998 and await the asset’s call the following morning.

Boone traveled to London on 11 September, checking his luggage at the airport, and carrying a black canvas bag that appeared to be a laptop computer case; the luggage and computer case were with Boone when he checked into the hotel in London.

On the morning of 12 September 1998, the asset telephoned Boone at the hotel and instructed him to come to a second hotel. There, Boone met the asset for approximately four hours and forty-five minutes. The asset specifically identified himself to Boone as a KGB/SVRR officer, explaining that Boone’s previous contact with the KGB/SVRR officer (Igor) had retired and was no longer available but that the asset had reviewed Boone’s KGB/SVRR file and had been tasked to recontact Boone. Boone’s response was, “I’m at your disposal.” Boone then freely provided the asset with specific details of how and why he volunteered to the Soviets and his contacts with them.

At the end of their meeting, Boone agreed to meet with the asset again on the following day to go over additional questions and to affirm future plans. Boone also agreed to prepare a written proposal of the information and assistance he felt he could provide to the KGB/SVRR in the future.

On 13 September 1998, Boone met with the asset at the second hotel for approximately one hour and forty-five minutes. Boone brought with him his luggage and the black canvas laptop computer case.

During this meeting, Boone provided more detailed information about having obtained classified materials for the KGB/SVRR during the period 1988-1991. Boone also brought and gave to the asset a handwritten page on which he had noted how he could provide information to the KGB/SVRR in the future.

Boone asked the asset if their business arrangement would be on a part-time or full-time basis. Boone suggested that if the KGB/SVRR had in mind a full-time position for him, he would be willing to move with his wife back to the United States to live. Boone suggested that he could set up a business at home as a cover for him to travel to various locations and to meet different people on behalf of the KGB/SVRR, if needed. Boone told the asset that he thought it might be cheaper this way. Boone included this suggestion on the proposal page that he gave to the asset.

At the end of this meeting, Boone accepted \$9,000 in prerecorded United States currency from the asset. Boone also agreed to travel to the United States on 2 October 1998 to meet again with the asset. Boone agreed to fly to Dulles International Airport, check into the Washington Dulles Airport Marriott Hotel located at the airport, meet with the asset the next day, and fly back to Germany on 4 October 1998.

While planning the 2 October 1998 meeting, Boone took a laptop computer out of the black canvas bag and logged on to check his schedule. The asset asked, "You have your computer here?" Boone replied, "I always take it with me." Boone entered the agreed-upon travel and meeting dates into his computer. When the asset sought to confirm that Boone had the asset's telephone number, Boone referred to the computer and stated that he had previously entered the number incorrectly; Boone corrected the number and told the asset, "Just so you know, you're listed as Georgi Bucharich (phonetic transcription) from Intertrust in London." This is neither the asset's name nor his affiliation, and the asset had not provided that name or affiliation to Boone.

Boone then left the asset and took a taxi to the airport. At the airport, Boone checked his luggage and carried the black canvas laptop computer case on board.

On 18 September 1998, Boone left a voice mail message at the telephone number provided by the asset. Boone advised that "the 2nd to the 4th might be difficult" for "the seminar," and that the "9th, 10th and 11th" would be preferable. Boone asked the asset to call him.

On 21 September 1998, the asset telephoned Boone, and they agreed that Boone would travel to Dulles on 9 October 1998 and check into the "hotel that we discussed," where the asset would call Boone at 9:00 am on 10 October 1998.

On 9 October 1998 Boone flew nonstop from Munich, Germany, to Dulles International Airport. FBI personnel observed Boone leave the airport with his luggage and a black canvas computer case similar to the one he carried to London for his meetings in September 1998 with the asset.

In their previous meeting, the asset instructed Boone to check into the Washington Dulles Airport Marriott Hotel upon arrival where Room 1431 had been reserved for him. The next day, Boone proceeded to another room in the hotel where he expected to meet the asset. Instead, an FBI Special Agent opened the door. The Special Agent identified herself and asked Boone to step inside. Boone was asked about his relationship with the asset, and he concocted a story about meeting him in the bar of the Hotel Russell in London in either August or September 1998. He added that they had agreed to meet in the future to discuss possible business deals. Boone agreed to summarize this information in a signed statement, which he did and handed it to the FBI Special Agent.

At that time, the Special Agent told Boone that she and the other Special Agent in the room were aware of the true reason Boone had come to meet with the asset and about his past relationship with the Russian Intelligence Service during 1988-1991. After hearing this, Boone asked, "Where do we go

from here?” It was explained to Boone that at the conclusion of the interview, he would be arrested. Boone then told his story to the Special Agents. At the conclusion of his story, Boone began writing a signed statement regarding his association with the Russian Intelligence Service. He was then arrested.

At his arraignment on 9 November 1998, Boone waived his right to a speedy trial on charges that he spied for the Soviet Union. On 18 December 1998, Boone pleaded guilty to conspiracy to commit espionage for the former Soviet KGB. In his guilty plea, Boone acknowledged that during 1988-1991 he delivered “highly classified documents” to agents of the KGB, the intelligence agency of the former Soviet Union.

On 26 February 1999, Boone was sentenced to 24 years and four months in prison. He agreed to forfeit \$52,000, including his retirement, and a hand-held scanner he used to copy documents.

The arrest of Boone was not without some political fallout. The Germans were upset that the FBI had “lured computer expert Boone to Washington and arrested him there, while deliberately circumventing German counterintelligence.” Willfried Penner (Social Democratic Party of Germany), chairman of the Bundestag’s Parliamentary Control Commission (known as the PKK) called the FBI operation “improper.” The German press also reported, “the annoyed Federal Office of Criminal Investigations [BKA] is currently investigating the scope of the espionage case.” The press further stated, “investigators searched Boone’s apartment and questioned his German wife. The FBI has already discreetly checked potential contact addresses in Bad Aibling and Bad Toelz, where US special units were stationed in the past.”² No further German media reporting appeared regarding the Boone case after November 1999.

Endnotes

¹ With the downfall of the Soviet Union in September 1991, the KGB was dismantled. The KGB’s First Chief Directorate, which was responsible for foreign intelligence operations, was renamed the SVRR—the Russian Federation foreign intelligence service, *Sluzhba Vneshney Razvedki Rossii*.

² *Munich Focus*, 2 November 1999, ‘Massive Ill Feeling’ Between FRG, US Counterintelligence.

Daniel King Case



Navy Petty Officer First Class Daniel King was apprehended on 28 October 1999 for passing data to the Russians—Article 92 of the Uniform Code of Military Justice—and espionage, which is Article 106 (a) of the Uniform Code of Military Justice. Navy spokesman Greg Smith said King, who has 18 years of service in the US Navy, was working with information gathered by American submarines lurking off the Russian coast when he allegedly sent secrets to the Russian Embassy in Washington in 1994. King was 40 years old at the time of his apprehension and is a native of Elyria, Ohio.

King was assigned to the Navy's intelligence operation in nearby Fort Meade, Maryland, at the time of his arrest. Navy officials said King's alleged disclosure was serious but not as damaging as earlier betrayals by Navy Warrant Office John Walker, who sold Russia critical Navy secrets and codes, or of Jonathan Pollard who handed suitcases full of US secrets to Israel.

A Navy official said King was promoted several times in his first seven years of service, but had been stuck at his current rank for eleven years. The official stated Mr. King's alleged crime may have been motivated by the perceived injustice of his stalled career.

Officials say the charges were filed after King failed a lie detector test he underwent as part of the routine process to renew his clearance to work

with highly secret materials. He was being held in pretrial confinement at the brig in Quantico, Virginia. According to the Navy spokesman, King admitted that he passed classified information about the US Navy submarine fleet on a computer disk to the Russian Embassy in 1994. He is also alleged to have discussed classified information with two women who had security clearances but were not cleared to receive information about the specific programs that he allegedly discussed.

According to the Associated Press, on 8 February 2000, the US Navy offered to drop espionage charges against King; however, King's attorney rejected the offer, saying that it contained details unfavorable to his client. According to one source, the Navy wanted to cut its losses and gain King's cooperation to determine the extent of damage to national security rather than risk losing at trial.

The offer to drop charges came after months of setbacks to the Navy's case that included defense accusations of security violations by the prosecutors and the investigating officer and a military appeals court twice ruling in the defense's favor, once ordering that prosecutors restart the case.

In October 2000, the Navy-Marine Court of Appeals chastised Navy prosecutors for delaying the proceeding for months by requiring that a monitoring agent be present at all meetings between King and his attorneys. The court deemed the Navy's actions unconstitutional and overturned the requirement.

In November, prosecutors lost a major witness when it was determined that he had been assigned to listen to private conversations between King and his attorneys for discussion of classified material. Then, in December, the court ruled in King's favor, ordering the prosecutors to restart the hearing after it found that the prosecutors and the presiding officer violated King's right to a public trial.

On 9 March 2001, the US Navy dropped all espionage charges against King. The officer overseeing the Navy's prosecution stated in a letter that, because of King's mental state during

questioning and the lack of corroborating evidence, he doubted the validity of King's confession. Another Navy source said the Navy was forced to drop espionage charges and two lesser charges because of the difficulty in protecting national security while upholding King's right to a public trial. King was released from custody in Quantico, Virginia, that same day.

After the dismissal of the case, Committee Chairman Richard C. Shelby (R-Ala.) denounced the Navy for a "bungled, botched" investigation and prosecution. Senator Shelby specifically criticized the prosecutor for mishandling the case and called for a hearing.

In unclassified testimony before the Senate Select Committee on Intelligence, the defense presented the facts of the case, including abuses by the Navy in its interrogations of King. These abuses included 20-hour interrogation sessions for 29 days, violations of federal rules on the use of polygraphs, and the denial of counsel to suspects. In addition, the defense disclosed a series of demonstrably false statements made to the media and Congress by the Navy in the aftermath of the case:

The Navy's Statement: "[W]hen a Sailor with access to the U.S. Navy's most sensitive programs repeatedly states that he betrayed the Navy's most crucial secrets, the Navy has an obligation to investigate."

The Truth: This widely disseminated statement is coupled with other suggestions that King admitted to espionage and compelled further inquiry. The record shows that it was not until eight days into the espionage investigation and after over 19 hours of interrogation that King signed any statement on espionage. The NCIS [Naval Criminal Investigative Service] began this investigation after a 'no opinion' result on a polygraph examination. It was the NCIS, not King, that probed fantasies of espionage and continued to interrogate exclusively on the subject of espionage. The NCIS should have simply given this sailor another polygraph after a common 'no opinion' result before triggering a full-fledge espionage investigation. The obvious misleading intent behind this statement is to suggest that Petty Officer King confessed immediately to such acts—a statement refuted on the record of signed statements, the audio tapes and other evidence in this case.

The Navy's Statement: "[T]he navy could not responsibly have chosen to simply ignore King's inability to pass his polygraph and subsequent incriminating statements."

The Truth: This statement was also part of the public release by the Navy after the dismissal of the case. As noted above, the statement does not mention that King did not fail his polygraph and did not make incriminating statements in triggering any investigation. King had a 'no opinion' result on a polygraph and repeatedly denied any espionage. Both military detailed counsels in this case had 'no opinion' results on their polygraph examinations and NCIS agents admitted that everyone in this field has a fantasy of espionage at some time in their career.

The Navy's Statement: "Petty Officer King also said he considered going to Russia to hurt the Navy by revealing sensitive information."

The Truth: This statement was also part of the public release by the Navy after the dismissal of the case. This statement is also knowingly misleading and false. During the interrogations, King admitted that he had been angry with the Navy at points in his 20-year intelligence career and that he had fantasized of being a spy. However, in the first three statements that he signed, King expressly stated that he never engaged in such acts and they were just passing flights of fancy. The Navy never mentions in its statement that this reference comes from what NCIS agents refer to as fantasies on the audio tapes. The Navy never mentions that King repeatedly emphasized that these were merely fantasies or that he expressly denied engaging in such conduct.

The Navy's Statement: "Petty Officer King also said . . . that he had committed serious security violations."

The Truth: This statement is also part of the public releases by the Navy. The Navy brought two charges for national security violations distinct from the espionage charge. Judge Winthrop summarily dismissed both of these charges as minor allegations that, even if true, should not have been submitted for prosecution. Judge Winthrop wrote: 'Although the evidence may surmount the low threshold of an Article 32 investigation, and that is by no means certain, I don't believe the government evidence on any of the charges in this case is strong. On the other hand, the defense evidence in extenuation and mitigation is significant.'

The wrongful disclosure allegations, and the related charges involving dereliction of duty and wrongful communication, are exemplary in this regard. The alleged violations occurred while the accused was on duty in a Sensitive Compartmented Information Facility (SCIF) in the presence of fellow service members with high level clearances. Each allegation is based on the recollection of one witness of events that occurred six and four years ago, respectively. Thus, on the merits, the government has one witness who will be required to rely on memory for events that occurred several years ago. With respect to extenuating and mitigating circumstances, it must be emphasized that the alleged disclosures occurred in secure areas to personnel that otherwise had high level clearances, but not access to the specific program in question. Thus, the threat to national security from these alleged violations was minimal. Furthermore, one witness did not take the disclosure seriously, while the other witness considered the information helpful in performing her job. It appears in both cases that the accused was disclosing the information to assist others in performing their duties. These facts constitute strong extenuating and mitigating evidence.

The Navy brought no other charges of national security violations. Ironically, the defense has detailed over three dozen proven violations of national security rules in this case by Navy and NCIS officials, including the identical violations made against King. Some of these unauthorized disclosures occurred in unsecured locations, like hotel rooms, and involved entirely uncleared individuals.

The Navy's Statement: "King failed multiple additional polygraph examinations, all of which were conducted in accordance with strict Department of Defense guidelines."

The Truth: At no point in the numerous statements issued by the Navy or the NCIS is there an admission that King did not fail his first polygraph examination but had a common 'no opinion' result. He continued to have such results on the second and third days of interrogation. The suggestion that these polygraphs met professional standards is laughable.

First, the NCIS agents never inquired about King's use of various drugs, some of which were seized in his room. King was openly taking over-the-counter drugs for weightlifting and weight-loss as well as drugs for medical conditions. These drugs can heighten responses and produce exaggerated responses to stressful questions.

Second, the NCIS continued to interrogate King for weeks while calling him a spy. He would be moved from highly prejudicial and stressful interrogations into these tests. The audio tapes in this case show King weeping and sobbing. He asks to go to sleep but is told to continue with the

interrogations. The agents lied to King and stated that he had failed polygraph examinations where he actually produced a "no opinion" result. In polygraph examinations, such lies undermine the results. By telling someone falsely that they failed, you guarantee that the person will elevate on the questions in anticipation on later examinations.

Third, from the first day, the agents forced King to repeatedly repeat prior fantasies and dreams of espionage. The agents repeatedly had King write down the fantasies and sign them as statements. King is heard on these tapes having an increasing difficulty in distinguishing fantasy from reality. Deposed agents admitted that he appeared to be struggling with what was real and what was dream during the interrogations. DoD regulations expressly forbid specific acts in the King case, which can be found in the last section of Professor Turley's unclassified testimony.

The Navy's Statement: "The interviews were reasonable, relaxed, and many were at the request of King."

The Truth: This is also from the public statement of the Navy. This statement is knowingly false. The audio tapes in this case show King weeping and sobbing. During 19-hour interrogations, King asked to go to sleep but is told to continue. The NCIS continues interrogations for 29 days. At times, King is shouting, 'I don't know what I'm supposed to give you' over and over at the agents as they press him for a signed confession. Moreover, it is noteworthy that King seeks the assistance of a psychologist for hypnosis on the videotaped interview with NCIS psychologist Dr. Michael Gelles. After his return to the United States, King was clearly trying to find a way to distinguish fantasy from reality. He told Gelles that he had no memory of the espionage facts but says that the polygraph examinations prove that he must have done something—a clear misconception that neither Gelles nor the agents correct.

The Navy's Statement: "King never told NCIS he wanted a lawyer, and he never asked for a lawyer."

The Truth: This is also part of the official statement released by the Navy and the NCIS. It is knowingly and demonstrably false. King asked for an attorney on October 5, 1999. Documents in the case establish at least two additional invocations of his right to counsel. On October 8, 1999, King signs a waiver of his right to remain silent but specifically invokes his right to counsel. King initials his statement that 'I do wish to have my lawyer present during the polygraph examination.' In a later waiver form, King again clearly asks for an attorney and again signed a statement (and initials an invocation), stating "I do desire to have my lawyer present during the polygraph examination."

No lawyer was ever produced by the NCIS, which continued to do polygraph examinations with long interrogations before and after the tests. Under *Edwards v. Arizona*, 451 U.S. 477 (1981), an attorney should have been supplied to King and interrogations suspended immediately when he asked for a lawyer on October 5, 1999. After the Navy and the NCIS issued these false statements, the defense released the documents showing invocations of counsel. The response of the Navy was that these were merely ‘typographical errors’ despite the fact that King both signed the form and initialed the specific language added on the invocation.

Previously, however, in defense of its conduct in the case, the Navy has repeatedly emphasized that ‘King reviewed each statement, made the changes that he wanted to make, and signed each statement . . . He swore to the voluntariness and truthfulness of each statement.’ Vernon Loeb & Walter Pincus, “Pentagon Probes Spy Case Navy Dropped Against Sailor,” *The Washington Post*, March 29, 2001 (statement of LCDR Cate Mueller, spokesperson for the United States Navy).

The Navy’s Statement: “*The Naval Criminal Investigative Service did not have further contact with King after he was ordered into pretrial confinement on October 28, 1999.*”

The Truth: This was also part of the public statement of the Navy and the NCIS. This statement was part of the argument that King was not in custody until he was placed in the brig. King was under 24-hour guard and moved from safe house to safe house in Guam. He was told that he would be shot if he attempted to escape. He was required to shower and go to the bathroom in the view of agents. However, putting aside the obvious elements of custody, neither the Navy nor the NCIS has ever revealed that military courts rejected this argument.

The Navy-Marine Court of Criminal Appeals twice stated that King was in custody starting October 2, 1999, when he was placed in the first safe house. The Navy did not contest this finding in an appeal to the Court of Appeals for the Armed Forces. Yet, after appellate courts have already decided this issue, the Navy and the NCIS continue to release false information to attempt to mitigate their misconduct in the case.

What is equally disturbing is that even the affirmative statement regarding the cessation of NCIS interrogations or further contact is false. The defense has sign-in sheets from the Quantico brig showing that, after King was placed in the brig, interrogations continued. The log shows NCIS agent Kenny Rogers signing in for an interrogation of King on October 31, 1999, three days after he was placed in the brig. This interrogation was particularly outrageous

because prosecutors with the assistance of the NCIS conducted it without defense counsel.

The Navy’s Statement: “*There was corroborating evidence in this case of espionage.*”

The Truth: As noted earlier, there was a torrent of leaks and false statements given to the media in this case. All these facts were attributed to specific spokespersons or confidential sources ‘close to the investigation.’ In March, the defense was asked to respond to a statement made by CDR Mark E. Newcomb. With the case still pending, CDR Newcomb told CBS *Sixty Minutes* that there was actually an abundance of corroborating evidence of espionage in the case.

The defense immediately wrote to CDR Newcomb on March 8, 2001 and demanded an explanation. Since no such evidence had been presented in the proceedings, the statement was either false or the government was again withholding evidence. CDR Newcomb wrote back to state that all possible corroborating evidence had been disclosed to the defense and the military judge. No corroborating evidence was being withheld. The only piece of evidence that the Navy could even offer as corroborating was a log that would be rejected in any court as corroborating evidence in this case.

Yet, Judge Winthrop was extremely critical of the absence of corroborating evidence in the case and stated that such evidence did not seem to even meet the standard of “slight” evidence of corroboration. Judge Winthrop stated that, even if King’s statement was found to be voluntary, “I question whether the mere existence of the daily log provides independent evidence of an ‘essential fact’ of the confession, i.e., the act of espionage.” In fact, the classified evidence in this case contains a great deal of exculpatory evidence including the audio tapes and investigative reports that find no evidence that King’s account actually occurred.

Stanislav Gusev



386152AI 8-02

STANISLAV GUSEV

On 8 December 1999, the FBI detained Russian intelligence officer, Stanislav Gusev, as he was recording transmissions from a bug implanted in a piece of chair rail, in a conference room within the Department of State headquarters building. Gusev's detention capped a six-month investigation that began when the FBI spotted the Russian intelligence officer loitering near the State Department.

Following surveillance and observation of Gusev, technical countermeasures discovered the remotely activated device in the conference room. Gusev was declared persona non grata and was required to leave the United States.

The FBI and State Department continue to investigate who was responsible for planting the bug and what sensitive materials discussed in the conference room may have been compromised. Recreating the extent to which Russian intelligence or other personnel may have had access to the room in question has been complicated by the fact that, from 1992 until August 1999, there were no escort requirements for Russian (or other foreign) visitors to the State Department.

George Trofimoff



386153AI 8-02

GEORGE TROFIMOFF

George Trofimoff, a.k.a. George Von Trofimoff, "Antey," "Markiz," and "Konsol," was born in Germany to Russian émigrés and became a naturalized US citizen in 1951. He enlisted in the US Army in 1948 and received a commission in the US Army Reserve in 1953. He was honorably discharged from active duty in 1956 and retired from the US Army Reserves with the rank of colonel in 1987. From 1959 through 1994, Trofimoff was employed by the US Army as a civilian working in military intelligence—primarily in Germany.

From 1969 to 1994, Trofimoff was the Chief of the US Army Element at the Nuernberg Joint Interrogation Center (JIC). As the chief, he had access to all of JIC's classified information. Among the classified documents related to US national defense that were maintained at the Nuernberg JIC were:

- Intelligence objectives listing current intelligence information required by the United States.
- Intelligence priorities for strategic planning that identified and ranked the current intelligence needs of the US military.
- Soviet and Warsaw Pact order-of-battle documents detailing the United States' current knowledge of Soviet and Warsaw Pact military organizations and capabilities.

- Collection Support Briefs on specific topics, such as the current chemical and biological warfare threat posed by the Soviet Union and the Warsaw Pact allies and others.
- Intelligence Information Reports that responded to identified intelligence collection requirements obtained from various sources, including interviews of refugees and defectors.

As a child in Germany, Trofimoff was raised with Igor Vladimirovich Susemihl, a.k.a. “Zusemihl” and “Iriney,” who was also the son of Russian émigrés. Trofimoff considered Susemihl to be his brother. Beginning in the 1960s, Trofimoff and Susemihl met often and maintained a close personal relationship.

Susemihl was a priest of the Russian Orthodox Church who served as Archbishop of Vienna and Austria and Temporary Archbishop of Baden and Bavaria. He later served as Metropolitan of Vienna and Austria and resided in the vicinity of Munich, Germany, until his death in 1999.

In 1969, after Trofimoff became the chief of the US Army Element at the Nuernberg JIC, Susemihl recruited him for the KGB. The KGB and later the SVRR—the successor to the KGB—assigned Trofimoff the codenames “Antey,” “Markiz,” and “Konsol.” They also assigned the codename “Ikar” to Susemihl.

From at least 1969 to about spring 1995, Trofimoff:

- Secretly took classified documents relating to the national defense from the Nuernberg JIC and passed them to the KGB.
- Secretly photographed US documents relating to the national defense.
- Purchased a Minox camera at the KGB’s direction but gave it to the KGB through Susemihl because “it was too dangerous to have.”
- Stored boxes of exposed film in his home until he could deliver them to Susemihl or to KGB officers.

- Traveled to Bad Ischi, Hallein, Zell am See, and near St. Johann—all in Austria—to meet with KGB officers. The KGB officers he met have been identified as Anatoliy Tikhonovich Kireyev, Victor Alesandrovich Chernyshev, and Yuriy Vasilyevich Lysov.
- Received from Susemihl and KGB officers cash payments and bonuses totaling approximately 90,000 deutsch marks.
- Used an oral recognition signal—called a parole—when he met with a KGB officer.

For his work on behalf of the KGB, Trofimoff received the Order of the Red Banner, which is the oldest Soviet award. It is presented to Soviet citizens and noncitizens for special bravery, self-sacrifice, and courage displayed in the defense of the Soviet homeland, including special bravery and courage displayed in accomplishing special assignments and in supporting the state security of the Soviet Union. Despite the awards, Trofimoff allegedly thought he still was owed money by the Russians.

In 1994, the German authorities arrested Trofimoff and Susemihl, but the case was dropped because of German concerns about the statute of limitations law in that country. In 1995, Trofimoff retired from the military after serving 35 years and moved to Brevard County in Florida where he bought a home in a gated community. Because there is no statute of limitations against espionage in the United States, the FBI took up the case.

After a seven-year investigation, the FBI conducted a sting operation against Trofimoff and secretly recorded the meetings. An FBI agent posing as a Russian intelligence officer contacted Trofimoff and offered to pay him the rest of what he was owed. During a series of meetings between Trofimoff and the undercover FBI agent at a hotel in Melbourne, Florida, Trofimoff described his spying activities in detail. On 14 June 2000, when Trofimoff appeared at the West Shore Hilton in Tampa, the FBI arrested him.

Trofimoff’s trial began on 6 June 2001. One of the

most damaging witnesses against Trofimoff was a British intelligence officer who provided testimony on information received from Vasili Mitrokhin, a Russian intelligence officer who defected in 1992. Mitrokhin smuggled information he had copied from KGB files out of KGB headquarters and hid it. After Mitrokhin defected, he gave his notes to British intelligence.

Testifying under the name of John Doe, the British intelligence officer acknowledged that Trofimoff's name was not in any of the KGB notes obtained from Mitrokhin but that the information concerning a US intelligence officer who became an "extremely valuable agent" for the KGB matched that of Trofimoff. The notes described a US military intelligence officer in the same unit where Trofimoff served who was recruited with the help of a Russian Orthodox Church priest. The spy, who was identified only by the codenames "Markiz," "Konsul," and "Antey," provided documents that were disseminated to top Soviet leaders, including former KGB chairman Yuri Andropov.

According to the British intelligence officer, the KGB kept count of the thousands of documents provided to them, noting titles of some highly sensitive reports detailing what the United States knew and didn't know about Soviet military capabilities. Mitrokhin's notes identified the spy as the leader in the 66th Military Intelligence Group—the unit where Trofimoff spent his career as an Army civilian employee.

The notes also showed that the spy's codename changed periodically, but the new codenames were accompanied by a description that didn't change. Markiz, Konsul, and Antey all were described as members of the 66th Military Intelligence Group and associated with another spy with the codename Ikar.

Mitrokhin's notes also identified Ikar as a Russian Orthodox priest who lived in Vienna and often traveled to East Germany and Moscow, where he could easily deliver information to the KGB. A KGB officer using the cover of a diplomat at the Soviet embassy in Vienna managed the two spies.

In late June 2001, Trofimoff was found guilty of espionage. On 27 September 2001, U. S. District Judge Susan Bucklew sentenced Trofimoff to life in prison.

George Trofimoff Affidavit

UNITED STATES DISTRICT COURT MIDDLE DISTRICT OF FLORIDA TAMPA DIVISION

CASE NO. 8:00-CR-197-T-24C

UNITED STATES OF AMERICA V.

**GEORGE TROFIMOFF,
a/k/a George Von Trofimoff,
a/k/a "Antey," a/k/a "Markiz," a/k/a
"Konsul"**

INDICTMENT

The Grand Jury charges:
COUNT ONE

A. INTRODUCTION

At all times relevant to this indictment:

1. The defendant, GEORGE TROFIMOFF, a/k/a George Von Trofimoff, a/k/a "Antey," a/k/a "Markiz," a/k/a "Konsul," was born in Germany to Russian émigrés, and became a naturalized United States citizen in 1951. He enlisted in the United States Army in 1948 and received a commission in the United States Army Reserve in 1953. He was honorably discharged from active duty in the United States Army in 1956, and retired from the United States Army Reserve with the rank of Colonel in 1987. From 1959 through 1994, TROFIMOFF was employed by the United States Army as a civilian working in military intelligence, serving primarily in Germany.
2. Pursuant to Executive Order 12958 and its preceding Orders, information, the unauthorized disclosure of which could reasonably be expected to cause "damage to national security," must be classified as CONFIDENTIAL and properly safeguarded. Information, the unauthorized disclosure of which reasonably could be expected to cause "serious damage to the national security,"

-
- must be classified as SECRET and properly safeguarded. Information, the unauthorized disclosure of which could reasonably be expected to cause “exceptionally grave damage to the national security,” must be classified as TOP SECRET and properly safeguarded.
3. Throughout his career with the United States Army, TROFIMOFF held SECRET and TOP SECRET clearances, and received periodic briefings and acknowledged his responsibilities in handling classified information.
 4. The United States, the Federal Republic of Germany, Great Britain, and others were member nations of the North Atlantic Treaty Organization (NATO), which provided for a common defense against the threat of military aggression.
 5. Until in or around 1991, the principal military threat to the NATO countries was from the Union of Soviet Socialist Republics (Soviet Union) and its Warsaw Treaty organization (Warsaw Pact) allies, which included German Democratic Republic (East Germany), the Polish People’s Republic, the People’s Republic of Hungary, the Czechoslovak Socialist Republic, and the People’s Republic of Bulgaria.
 6. Since in or around 1991, NATO has guarded against potential threats from former republics of the Soviet Union, including the Russian Federation, and their allies.
 7. As a member of NATO the United States had a military intelligence presence in Western Europe, including the 66th Military Intelligence Group (MIG).
 8. A mission of the 66th MIG was to work together with the military intelligence services of other countries in collecting intelligence about Warsaw Pact countries. One source of this intelligence was interviews of refugees and defectors from Warsaw Pact countries. Some such interviews were conducted by military intelligence personnel assigned to Joint Interrogation Centers (JIC).
 9. A JIC at Nuernberg in the Federal Republic of Germany was staffed by United States Army personnel as well as other United States, German, British, and French military personnel. From 1969 to 1994, the defendant GEORGE TROFIMOFF was the Chief of the United States Army Element at the Nuernberg JIC,
 10. The United States Army Element at the Nuernberg JIC received classified information, including documents produced by members of the United States intelligence community such as the Defense Intelligence Agency.
 11. As Chief of the United States Army Element at the Nuernberg JIC, TROFIMOFF had access to all classified information, including documents, received by and produced by the United States Army Element.
 12. Among the classified documents related to the national defense of the United States which were maintained at the Nuernberg JIC were the following:
 - (a) Intelligence Objectives, which listed current intelligence information required by the United States.
 - (b) Intelligence Priorities for Strategic Planning, which identified and ranked the current intelligence needs of the United States military.
 - (c) Soviet and Warsaw Pact Order of Battle documents which detailed the United States’ current state of knowledge of Soviet and Warsaw Pact military organizations and capabilities.
 - (d) Collection Support Briefs on specific topics such as the current chemical and biological warfare threat posed by the Soviet Union and its Warsaw Pact allies and others.
 - (e) Intelligence Information Reports, which were reports of information responsive

-
- to identified intelligence collection requirements, obtained from various sources including interviews of refugee and defectors.
13. The Committee for State Security of the Soviet Union (Komitet Gosudarstvennoy Bezopasnosti, referred to as the KGB) was the principal intelligence and counterintelligence service of the Soviet Union and was organized into Chief Directorates, Departments and Services. The KGB viewed the United States as the principal adversary, or main enemy, of the Soviet Union, and as the KGB's primary intelligence target.
14. Among the KGB's missions was counterintelligence, which was aimed at identifying and counteracting the threat posed to the security of the Soviet Union by hostile intelligence services, such as those of the United States. This mission required the KGB to obtain intelligence information about the state of adversaries' knowledge about the military preparedness of the Soviet Union and its Warsaw Pact allies.
15. A method by which the KGB obtained intelligence information about its adversaries was to recruit persons having authorized access to such intelligence information to provide it to the KGB, thereby giving the KGB the opportunity to identify, penetrate, and neutralize potential threats to the Soviet Union, and to conduct denial and deception.
16. The Russian Orthodox Church was an organized religious institution within the Soviet Union and had churches and officials, including clergy, both within the Soviet Union and abroad.
17. The KGB exploited the Russian Orthodox Church and its officials, including clergy, in furtherance of the missions of the KGB.
18. Igor Vladimirovich Susemihl, a/k/a Zusemihl, also called "Iriney," was a priest of the Russian Orthodox church who served as the Archbishop of Vienna and Austria and Temporary Archbishop of Baden and Bavaria, and later served as Metropolitan of Vienna and Austria, and who resided in the vicinity of Munich, Federal Republic of Germany, until his death in 1999.
19. The defendant GEORGE TROFIMOFF was raised in Germany with Susemihl, who was also the son of Russian émigrés, and TROFIMOFF considered Susemihl to be his "brother." Beginning during the 1960s, TROFIMOFF and Susemihl met often and maintained a close personal relationship.
20. In or about 1969, after the defendant GEORGE TROFIMOFF became the Chief of the United States Army Element at the Nuernberg JIC, Susemihl recruited him into the service of the KGB.
21. Within the KGB, the First Chief Directorate (FCD) was primarily responsible for foreign intelligence.
22. Within the FCD, Directorate K was responsible for the KGB's counterintelligence mission abroad.
23. KGB officers who had counterintelligence responsibilities often operated abroad from diplomatic missions of the Soviet Union. These intelligence officers worked for Line KR of Directorate K.
24. The Order of the Red Banner is the oldest Soviet award and was presented to citizens and non-citizens for special bravery, self-sacrifice, and courage displayed in the defense of the socialist homeland, including special bravery and courage displayed in accomplishing special assignments, and special bravery and courage displayed in support of the state security of the Soviet Union.
25. Since 1992, the Russian Foreign Intelligence Service (Sluzhba Vneshney Rezvedki Rossii, referred to as the SVRR) has been the successor to the KGB as the foreign intelligence service of the Russian Federation.

B. The Agreement

26. Beginning on or about an unknown date which was at least 1969, and continuing through in or around the spring of 1995, both dates being approximate and inclusive, in the Federal Republic of Germany, the Republic of Austria, and elsewhere outside the jurisdiction of any State or district of the United States, the defendant, GEORGE TROFIMOFF, a/k/a George Von Trofimoff, a/k/a "Antey," a/k/a "Markiz," a/k/a "Konsul," did knowingly and willfully combine, conspire, confederate, and agree with various other persons whose names are both known and unknown to the Grand Jury, to knowingly and willfully communicate, deliver, and transmit and to attempt to communicate, deliver, and transmit directly and indirectly to a foreign government, that is, the Union of Soviet Socialist Republics, and to representatives, officers, agents, and employees thereof, documents, photographs, photographic negatives, and information relating to the national defense of the United States, with intent and reason to believe that the same would be used to the injury of the United States and to the advantage of a foreign nation, in violation of Title 18, United States Code, Section 794(a).

C. The Manner and Means of the Conspiracy

27. It was part of the conspiracy that agents, representatives, officers, and employees of the KGB/SVRR would and did recruit individuals who had access to classified information relating to the national defense of the United States to obtain such information and transmit it to agents, representatives, officers, and employees of the KGB/SVRR. The persons recruited to conduct such espionage were called "agents-in-place."

28. It was further part of the conspiracy that agents, representatives, officers, and employees of the KGB/SVRR would and did pay money-including regular cash payments, bonuses, and special payments - to their agents-in-

place, including the defendant GEORGE TROFIMOFF, in exchange for classified information relating to the national defense of the United States, including those documents described in Paragraph 12.

29. It was further part of the conspiracy that agents, representatives, officers, and employees of the KGB/SVRR would and did have meetings in the Federal Republic of Germany and the Republic of Austria with their agents-in-place for the purpose of obtaining classified information relating to the national defense of the United States, and in exchange would give these persons monetary payments and instructions for further espionage activities on behalf of the KGB/SVRR.

30. It was further part of the conspiracy that agents, representatives, officers, and employees of the KGB/SVRR would and did provide to their agents-in-place, and cause their agents-in-place to purchase, obtain, and use, equipment, including, but not limited to, photographic equipment and film, for the purpose of furthering their espionage activities on behalf of the KGB/SVRR.

31. It was further part of the conspiracy that agents, representatives, officers, and employees of the KGB/SVRR would and did cause its agents-in-place to secretly carry classified documents relating to the national defense of the United States, away from the locations where they were supposed to be kept, by utilizing briefcases and bags.

32. It was further part of the conspiracy that agents, representatives, officers, and employees of the KGB/SVRR would and did utilize agents and apparently innocent persons to spot, assess, and co-opt targets for recruitment as agents-in-place, and to introduce those persons to agents, representatives, officers, and employees of the KGB/SVRR.

33. It was further part of the conspiracy that officers and agents, representatives, officers,

and employees of the KGB/SVRR and their agents-in-place, and their agents-in-place, would and did use innocuous explanations for their activities on behalf of the KGB/SVRR.

34. It was further part of the conspiracy that the KGB/SVRR would and did protect its agents-in-place through disinformation and other means.
35. It was further part of the conspiracy that the KGB/SVRR would and did assign to its agents code names which were periodically changed. The KGB/SVRR assigned to the defendant, GEORGE TROFIMOFF, the code names "Antey," "Markiz," and "Konsul," and assigned to Igor Susemihl the code name "Ikar."
36. Aleksandr Vasilyevich Blagov, a/k/a "Vlagov," was a KGB/SVRR officer who operated out of Soviet/Russian diplomatic missions in Europe and maintained contact with Igor Susemihl and others in furtherance of the missions of the KGB/SVRR.
37. It was further part of the conspiracy that agents, representatives, officers, and employees of the KGB/SVRR would and did continue to communicate with their agents-in-place after the agents-in-place had ceased providing intelligence information to the KGB/SVRR, in order to ensure continued loyalty and protection.
38. It was further part of the conspiracy that the defendant, GEORGE TROFIMOFF, and others would and did misrepresent, conceal, and hide, and cause to be misrepresented, concealed, and hidden, the acts done in furtherance of the conspiracy.

D. Overt Acts

39. In furtherance of and to effect the objects of the conspiracy, the defendant, GEORGE TROFIMOFF, did commit various overt acts, including but not limited to, the following: (Unless otherwise stated, these overt acts each occurred between at least 1969 and December 1994.)

- (1) GEORGE TROFIMOFF secretly took classified United States documents relating to the national defense away from the Nuernberg JIC.
- (2) GEORGE TROFIMOFF secretly photographed classified United States documents relating to the national defense.
- (3) GEORGE TROFIMOFF secretly removed and replaced staples in classified United States documents relating to the national defense in order to photograph the documents' contents.
- (4) GEORGE TROFIMOFF secretly returned classified United States documents relating to the national defense to the Nuernberg JIC.
- (5) GEORGE TROFIMOFF purchased a Minox camera at the direction of the KGB, but "turned it back in" through Igor Susemihl because "it was too dangerous to have."
- (6) GEORGE TROFIMOFF used a double-frame camera to photograph the contents of classified United States documents relating to the national defense.
- (7) GEORGE TROFIMOFF made and used a device to place documents while he photographed them, "so the page would fit exactly."
- (8) GEORGE TROFIMOFF possessed two goose neck lamps in 1994.
- (9) GEORGE TROFIMOFF purchased film.
- (10) GEORGE TROFIMOFF put rolls of exposed film back into their original boxes and glued the boxes shut.
- (11) GEORGE TROFIMOFF stored boxes of exposed film at his home until he delivered them to Igor Susemihl or to KGB officers.

-
- | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>(12) GEORGE TROFIMOFF hand carried boxes of exposed film to Igor Susemihl.</p> <p>(13) GEORGE TROFIMOFF hand carried boxes of exposed film to KGB intelligence officers.</p> <p>(14) GEORGE TROFIMOFF maintained a regular relationship with and had frequent contacts with Igor Susemihl.</p> <p>(15) GEORGE TROFIMOFF traveled to Amstetten, Austria, and met with a KGB officer.</p> <p>(16) GEORGE TROFIMOFF traveled to Zell am See, Austria, and met with a KGB officer.</p> <p>(17) GEORGE TROFIMOFF traveled to Bad Ischl, Austria, and met with a KGB officer.</p> <p>(18) GEORGE TROFIMOFF traveled to Hallein, Austria, and met with a KGB officer.</p> <p>(19) GEORGE TROFIMOFF traveled to in or around St. Johann, Austria, and met with a KGB officer.</p> <p>(20) GEORGE TROFIMOFF met with KGB officer Anatoliy Tikhonovich Kireyev, a/k/a Kireev.</p> <p>(21) GEORGE TROFIMOFF met with KGB officer Victor Aleksandrovich Chernyshev, a/k/a Tschernyshev.</p> <p>(22) GEORGE TROFIMOFF met with KGB officer Yuriy Vasilyevich Lysov.</p> <p>(23) GEORGE TROFIMOFF turned over to the KGB photographs of documents from the JIC which he believed would be of value to the KGB and could not be traced to him.</p> <p>(24) GEORGE TROFIMOFF received periodic</p> | <p>cash payments in Deutschmarks from Igor Susemihl, and from KGB officers.</p> <p>(25) GEORGE TROFIMOFF received cash bonuses from the KGB.</p> <p>(26) GEORGE TROFIMOFF received approximately 90,000 Deutschmarks from KGB.</p> <p>(27) GEORGE TROFIMOFF used an oral recognition signal or statement, called a “parole”, when he met with a KGB officer.</p> <p>(28) GEORGE TROFIMOFF concealed from his wives his espionage activities and the true nature of the money he received from the KGB.</p> <p>(29) GEORGE TROFIMOFF failed to report his relationship with Igor Susemihl, to the United States Army, as he was required to do.</p> <p>(30) In or around December 1994, GEORGE TROFIMOFF and Igor Susemihl told authorities in Germany that money TROFIMOFF received from Igor Susemihl was personal loans.</p> <p>(31) In or after December 1994, GEORGE TROFIMOFF discarded a tripod.</p> <p>(32) GEORGE TROFIMOFF was awarded the Order of the Red Banner.</p> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

E. Venue

Venue is obtained by Title 18, United States Code, Section 3238.

All in violation of Title 18, United States Code, Section 794(c).

Forfeitures

1. The allegations contained in Count One of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures, pursuant to the provisions of Title 18, United States Code, Section 794(d).
2. From his engagement in any or all of the violations alleged in Count One, punishable by imprisonment for more than one year, the defendant shall forfeit to the United States, pursuant to Title 18, United States Code, Section 794(d)(1)(A) and (B), all of his interest in:
 - a. Property constituting and derived from any proceeds the defendant obtained, directly or indirectly, as a result of such violations; and
 - b. Property used and intended to be used in any manner or part to commit or to facilitate the commission of such violations.
3. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:
 - a. cannot be located upon the exercise of due diligence;
 - b. has been transferred, sold to, or deposited with, a third party;
 - c. has been placed beyond the jurisdiction of the Court;
 - d. has been substantially diminished in value; or
 - e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated in Title 18, United States Code, Section 794(d)(3), to seek forfeiture of any other property of said defendant up to the value of the above forfeitable property.

All in violation of Title 18, United States Code, Section 794.

A TRUE BILL,

FOREPERSON

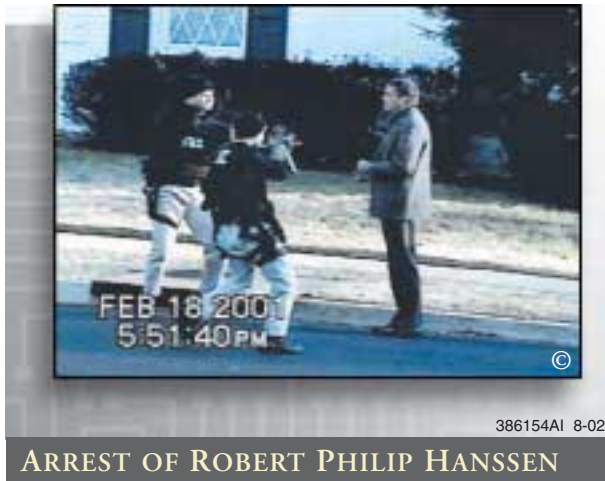
DONNA A. BUCELLA
United States Attorney

WALTER E. FURR, III
Assistant United States Attorney
Chief, Narcotics Section

LAURA A. INGERSOLL
Senior Trial Attorney
Internal Security Section
United States Department of Justice

Robert Philip Hanssen

The FBI arrested Robert Philip Hanssen, a 27-year veteran of the bureau, on 18 February 2001 at his home in Vienna, Virginia, after he allegedly dropped off a package of classified information at a nearby park. Prosecutors said Hanssen began spying for Russia in 1985, but Hanssen's lawyer said that his espionage career actually began in 1979. Hanssen later confirmed this date. After a hiatus, he renewed his espionage activities when he sent a letter to the KGB in 1985. He passed on highly classified information to the Russians over the years. He also identified three Russian intelligence agents who were working for the United States.



After the usual postulating by both sides—the Department of Justice and Hanssen's lawyer—prior to an actual trial, a plea agreement was reached. On 6 July 2001, Hanssen publicly admitted that he engaged in a 15-year-long conspiracy to commit espionage against the United States. In the plea agreement accepted by the judge, Hanssen pleaded guilty to that conspiracy, to 13 different acts of espionage and to one count of attempted espionage.

Under the plea agreement, Hanssen received a life prison sentence with no possibility of parole. The agreement also required Hanssen to submit to extensive debriefings by the US Intelligence Community.

Hanssen's initial letter with the names of three Russia officers spying for the United States certainly caused the KGB to accept his bona fides quickly. Although the KGB's CIA spy Aldrich "Rick" Ames had previously provided the same names to the KGB, his letter coming shortly after Ames made the identification only confirmed the guilt of the Russian officers. In addition, the information Hanssen passed to the KGB was of extremely high quality and that the KGB probably knew that he was a senior FBI officer with access to counterintelligence information.

Hanssen and his Russian intelligence handlers used simple, time-honored tradecraft to communicate with each other. No use was made of secret writing. Although Hanssen had substantial communications with the KGB about using sophisticated computer techniques for communications, they used no sophisticated communication devices or modern technology but relied on the US postal service, the telephone, and signal sites and deaddrops.

Well aware that the many unsuccessful American spies were caught when they telephoned the Soviet/Russian Embassy, Hanssen avoided calling there. He devised using the newspaper ad to trigger a call to a number not connected with the Soviets and, therefore, not under FBI surveillance. Even the letters and documents he mailed to the Soviets were sent to officers he knew were not under FBI letter coverage.

They did use computer diskettes for informational purposes only—Hanssen passing 26 diskettes to the KGB/SVR¹ and the KGB/SVR passing 12 diskettes to Hanssen. Hanssen also kept reminders of his clandestine appointments in his Palm III organizer, which is a hand-held personal digital assistant. The FBI determined that Hanssen's Palm III contained a reference to "ELLIS" and the date 18 February and the time 8:00. The term "ELLIS" is the KGB/SVR codename for the deaddrop site located in the area of Foxstone Park that was used seven times by "B," the KGB/SVR, or both.

During his espionage career, Hanssen sent 27 letters to the KGB/SVR, loaded 22 packages in deaddrops, and had two telephone conversations with KGB personnel. The KGB/SVR loaded 33 packages in deaddrops for Hanssen to unload. Signal sites were used to indicate when either Hanssen or the KGB/SVR loaded and unloaded the drops.

Hanssen's selection of Nottoway Park ("PARK/PRIME") as a deaddrop site clearly showed that Hanssen did his homework before embarking on his espionage career. His instructions as to the location, package preparation, signal locations, and signals were well prepared. Up until this time, the KGB had not used public parks but preferred to use rural areas for drop sites—like the one used with John Walker.

It is also interesting to note that just before Aldrich "Rick" Ames' return to the United States in 1992—the same year Hanssen drops contact with the KGB—the KGB gave Ames a drop site at Little Falls Branch Park ("BRIDGE"). Other drop sites given to Ames were also in parks—Langley Park ("Creek"), Rock Creek Park ("Ground"), and Wheaton Regional Park ("Pipe"). In 1991 the SVR and Hanssen also used Rock Creek Park as a drop site ("Grace") but only one time. Hanssen probably did not like using this site because it was outside Virginia and outside his pattern of movement. This demonstrates that the successful use of parks with Hanssen was not lost on the KGB/SVR.

For all their expertise in running successful spies over the years—the Walkers, Ames, Clyde Conrad—the KGB/SVR did not control the operation; Hanssen did. He never told them his name. His initial contact was an unsigned letter to the Soviets—the KGB called him "B." In a June 1986 letter to the KGB, Hanssen signs it "Ramon." Over a year later, he uses the name "R. Garcia" in the return address line.

In November 1987, Hanssen changes from R. Garcia to J. Baker—later he uses Jim Baker. He again changes the return address name over a year later—1 December 1988—to G. Robertson, but in August 1990 he reverts back to J. Baker. In 1992, Hanssen breaks contact with the SVR. In October 1999 the SVR leaves a letter for Hanssen in a drop,

but there is no further contact between the two. This obviously upsets Hanssen who writes to the SVR in March 2000 to complain about the silence from the SVR. He signs this letter Ramon Garcia as if to say to the SVR, Remember me!

On three occasions, the KGB/SVR suggested that Hanssen meet with them abroad. The KGB probably suggested meeting overseas as a way to put a name and a face to their agent, get to know him personally, and to discuss future contact instructions and tasking. Also, the KGB suggested meeting outside the United States because they feel more secure in meeting an American agent beyond the surveillance reach of the FBI. The FBI's previous successes against them made the KGB reluctant to hold any personal meetings in the United States.

Each time a meeting outside the United States was raised, Hanssen rejected it. He told the KGB/SVR that foreign travel was a tipoff to counterintelligence of possible espionage activity.

Hanssen was concerned about his security. He not only changed the names he used on letters to the KGB/SVR but also periodically checked the FBI's Automated Case Support System (ACS) to determine if any of his activities came to the Bureau's attention. An audit of Hanssen's use of ACS showed that he was a consistent user of the Electronic Case File (ECF) in particular and that he periodically conducted searches of the ECF database, using a wide variety of very specific search terms. Although some of Hanssen's ACS use appeared to have been related to his official responsibilities, he made a substantial number of ACS searches apparently directly related to his own espionage activities.²

Through these searches, Hanssen could retrieve certain FBI records that would indicate whether he or his KGB/SVR associates, or their activities or operational locations, were known to or suspected by the FBI and, thus, whether he was exposed to danger. For example, on the following dates, Hanssen searched the ECF for the following terms, limiting some of the searches to a specified period of time as indicated:

25 July 1997	Hanssen
30 March 1998	Dead Drop and KGB
18 May 1998	Dead Drop Dead Drop and Russia
6 July 1998	Dead Drop Dead Drop and Washington FISA and Cell Phone Hanssen
30 July 1998	9414 Talisman Dead Drop Dead Drop and Washington Double D Hanssen Robert P. Hanssen
3 September 1998	Robert Hanssen Robert P Hanssen Robert P. Hanssen
21 September 1998	'Dead Drop' 'Dead Drop' and Russia
13 October 1998	Dead Drop Dead Drop [Dates=08/01/1998-10/13/1998
27 October 1998	'Dead Drop' 'Dead Drop' and Washington 'Dead Drop' Washington
14 December 1998	Dead Drop Dead Drop and Washington
7 April 1999	Drop Site Drop Site and Russia.89
12 April 1999	Robert Hanssen Talisman Drive White Cedar Whitecedar Court
11 August 1999	CCTV and Virginia CCTV and Virginia[Dates=01/01/1999008/11/1999 Foxstone
17 August 1999	Dead Drop[Dates=01/01/1999-08/17/1999
30 August 1999	Dead Drop Dead Drop [Dates=07/01/1999-08/30/1999 September 2, 1999:CCTV CCTV and SVR 'Dead Drop' and SVR 'Dead Drop' SVR
28 September 1999	Drop Site Drop Site[Dates=10/01/1999-10/21/1999 Talisman
21 October 1999	Dead Drop[Dates=10/01/1999-10/21/1999
26 October 1999	Vienna and Virginia Vienna and Virginia and FCI[Dates=1/01/1999/10/27/1999]
27 October 1999	Dead Drop[Dates=1/09/1999-1/28/1999
3 November 1999	Foxstone Foxstone and Vienna Vienna and Drop Vienna and Drop and FCI[Dates=01/01/1999-11/4/1999 Vienna and Drop[Dates=01/06/1999-03/11/1999
15 November 1999	Dead Drop and Virginia Foxstone.90
13 January 2000	Dead Drop[Dates=01/01/2000-01/13/2000 Dead Drop[Dates=10/01/1999-12/31/1999
18 January 2000	Drop Site and Virginia SVR and Dead Drop Not GRU
14 March 2000	Dead Drop and SVR
31 March 2000	Dead Drop Dead Drop and Russia
22 May 2000	Talisman Drive
28 September 2000	Dead Drop and Washington
4 October 2000	Drop Site[Dates=08/01/2000-10/04/2000
13 November 2000	Dead Drop[Dates=10/01/2000-11/13/2000
21 December 2000	Dead Drop[Dates=10/01/2000-12/22/2000 Espionage[Dates=11/01/2000-12/21/2000
3 January 2001	Robert Hanssen
16 January 2001	Dead Drop[Dates=12/01/2000-01/15/2001 Espionage[Dates=11/01/2000-01/15/2001
19 January 2001	Dead Drop[Dates=12/01/2000-01/18/2001
22 January 2001	Dead Drop[Dates=01/01/2000-01/12/2001 Dead Drop[Dates=12/01/2000-01/22/2001 DeadDrop[Dates=01/01/2000-01/22/2001 Foxstone

Hanssen did tremendous damage to the FBI's counterintelligence program against the Russians by identifying FBI sources, providing information on the FBI Double Agent Program, and numerous FBI counterintelligence investigative techniques, sources, methods and operations, and FBI operational practices and activities targeted against the KGB/SVR. He also advised the KGB/SVR as to specific methods of operation that were secure from FBI surveillance and warned the KGB/SVR as to certain methods of operation that were subject to FBI surveillance. In addition, he disclosed to the KGB the FBI's secret investigation of Felix Bloch, a Foreign Service Officer, for espionage, which led the KGB to warn Bloch that he was under investigation, which completely compromised the investigation.

Hanssen also did immense damage to the US Intelligence Community (IC). He compromised numerous human sources and dozens of US Government classified documents. These documents pertained to the National MASINT (Measurement and Signature Intelligence) Program, the US Double Agent Program, and the US IC's Comprehensive Compendium of Future Intelligence Requirements. He passed a study concerning KGB recruitment operations against the CIA, an assessment of the KGB's effort to gather information concerning certain US nuclear programs, and a CIA analysis of the KGB's First Chief Directorate. He gave them a highly classified and tightly restricted analysis of the foreign threat to a specific-named highly compartmented classified US Government program and other classified documents of exceptional sensitivity.

He compromised US IC technical operations of extraordinary importance and value. This included specific electronic surveillance and monitoring techniques and precise targets of the US IC. In one case, he compromised an entire technical program of enormous value, expense, and importance to the US Government. In several other cases, he compromised the US IC's specific communications intelligence capabilities, as well as several specific targets. All in all, Hanssen provided the KGB/SVR more than 6,000 pages of documentary material.

Hanssen claimed that his decision to become a spy began when he was 14 years old and read Kim Philby's book entitled *My Silent War*. If his claim is true, he gained some insight into the espionage world, found it fascinating, and decided to he wanted to take part. He actually did try his hand at being a spy in 1979—just two years after he joined the FBI—when he sent a letter to the GRU offering his services. He communicated with them until 1982 when his wife discovered his activities and told him to stop. There has been no further media reporting on his work for the GRU or what he provided to them.

He obviously learned a great deal from this initial, undetected foray into being a double agent. Combined with his FBI training and knowledge, he was well prepared three years later when he contacted the KGB. Although financial vetting was given greater importance within the Intelligence Community based on the Ames case—for the money—this tool is not effective if an intelligence officer is receiving illicit payments, which he takes deliberate steps to hide. He used the funds he received from the KGB/SVR in such a way that it was not noticeable. He never purchased a house that drew attention and he drove older cars—unlike Ames who purchased an expensive home and bought himself a Jaguar.

Money was not the sole contributing factor in Hanssen's decision to be a spy. While the money probably helped him finance his children's private education, ego also played a role. He found the role of spy to be an adventure—alluring and exciting—that gave him a feeling of power and control. Like Philby, he apparently believed that he would influence the course of history. The three times in which the Soviets/Russians conveyed thanks or regards from the KGB Director seemingly reinforced this belief.

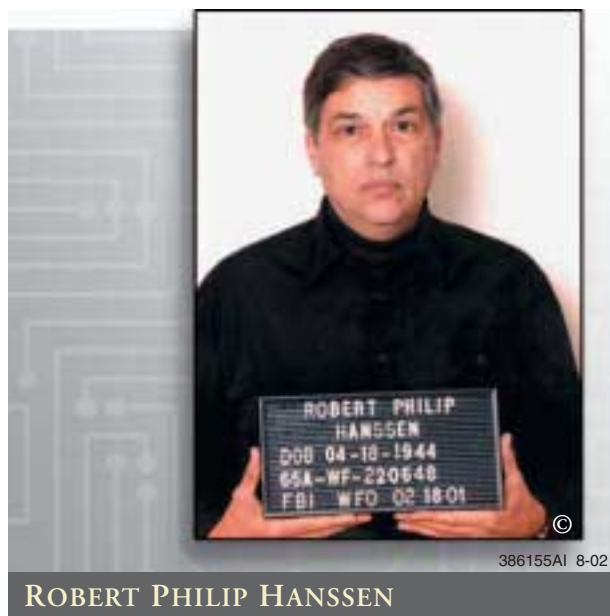
Despite not being able to personally meet with Hanssen, the Soviets/Russians seized opportunities to show that they valued his personal opinion and had faith in his ability to assess the local security environment. They told him on several occasions

that they wanted him to comment on information he provided so that they would not take any precipitous action to jeopardize his security.

In April 1989, the KGB presented several awards to KGB officers involved in the Hanssen espionage operation, including the highly coveted Order of the Red Banner, the Order of the Red Star, and the Medal for Excellent Service.

Hanssen's FBI Career

On 12 January 1976, Hanssen joined the FBI as a Special Agent. After initial training, he was assigned to the FBI Field Office in Indianapolis, Indiana, and served on a White Collar Crime squad at the Resident Agency in Gary, Indiana, until 1 August 1978. The next day Hanssen was assigned to the FBI Field Office in New York, New York, initially working on accounting matters in the field office's criminal division.



In March 1979, Hanssen was detailed to the New York Field Office's Intelligence Division to help establish the FBI's automated counterintelligence database in that office. At that time, this was a new automated database of information about foreign officials, including intelligence officers, assigned to

the United States. Hanssen left the New York Field Office on 10 January 1981.

On 12 January 1981 Hanssen was assigned to FBI Headquarters in Washington, DC, as a Supervisory Special Agent in the Intelligence Division. He was assigned to the Budget Unit, which managed the FBI's portion of the United States Intelligence Community's National Foreign Intelligence Program, and prepared budget justifications to Congress. This office had access to the full range of information concerning intelligence and counterintelligence activities involving FBI resources.

From August 1983 until September 1985, Hanssen was assigned to the Soviet Analytical Unit, which supported FBI FCI operations and investigations involving Soviet intelligence services, and provided analytical support to senior FBI management and the Intelligence Community. While at FBI Headquarters, Hanssen was assigned to the intelligence component of a particular highly compartmented classified US Government program. He also served on the FBI's FCI Technical Committee, which was responsible for coordinating technical projects relating to FCI operations.

On 23 September 1985, Hanssen was assigned to the Intelligence Division of the FBI Field Office in New York, New York, as supervisor of an FCI squad. He left New York to return to FBI Headquarters on 2 August 1987.

On 3 August 1987, he again served as a Supervisory Special Agent in the Intelligence Division's Soviet Analytical Unit. On 25 June 1990, Hanssen was assigned to the FBI Headquarters' Inspections Staff as an Inspector's Aide. In this assignment he traveled to FBI Field Offices, Resident Agencies, and FBI Legal Attache offices in US Embassies abroad.

On 1 July 1991, he returned to the Intelligence Division at FBI Headquarters. He served for six months in the Soviet Operations Section as a program manager in the unit responsible for countering efforts by the Soviets (and particularly

the KGB's Line X) to acquire US scientific and technical intelligence.

On 6 January 1992, Hanssen became Chief of the National Security Threat List (NSTL) Unit in the Intelligence Division (renamed the National Security Division, or NSD, in 1993) at FBI Headquarters. There he focused the Unit's efforts on economic espionage. He was temporarily assigned to the FBI's Washington Metropolitan Field Office (now called Washington Field Office) on 11 April 1994. In December 1994, he was reassigned to FBI Headquarters, in the Office of the Assistant Director for NSD.

Hanssen was detailed on 12 February 1995 to serve as the FBI's senior representative to the Office of Foreign Missions of the US Department of State (DOS/OFM). In that position he functioned as the head of an interagency counterintelligence group within DOS/OFM and as FBI's liaison to the State Department's Bureau of Intelligence and Research (DOS/INR).

Effective 13 January 2001, Hanssen was assigned to a newly created position in the Information Resources Division at FBI Headquarters in order that the FBI could more effectively monitor his daily activities without alerting him to the ongoing investigation of his activities.

Letters to the KGB/SVR

Hanssen resumed his spying activities when he mailed an envelope on 1 October 1985 to the residence of Viktor M. Degtyar in Alexandria, Virginia. Degtyar was a KGB Line PR (Political Intelligence) officer stationed at the Soviet/Russian Embassy in Washington, DC. The envelope was postmarked "Prince George's Co, MD." When he opened the envelope, he found an inner envelope, marked "DO NOT OPEN. TAKE THIS ENVELOPE UNOPENED TO VICTOR I. CHERKASHIN." At that time, Viktor Ivanovich Cherkashin was the Line KR (Counterintelligence) Chief at the Soviet Embassy.

Inside the inner envelope was an unsigned typed letter from the person whom the KGB came to call "B." The letter read in part as follows:

DEAR MR. CHERKASHIN:

SOON, I WILL SEND A BOX OF DOCUMENTS TO MR. DEGTYAR. THEY ARE FROM CERTAIN OF THE MOST SENSITIVE AND HIGHLY COMPARTMENTED PROJECTS OF THE U.S. INTELLIGENCE COMMUNITY. ALL ARE ORIGINALS TO AID IN VERIFYING THEIR AUTHENTICITY. PLEASE RECOGNIZE FOR OUR LONG-TERM INTERESTS THAT THERE ARE A LIMITED NUMBER OF PERSONS WITH THIS ARRAY OF CLEARANCES. AS A COLLECTION THEY POINT TO ME. I TRUST THAT AN OFFICER OF YOUR EXPERIENCE WILL HANDLE THEM APPROPRIATELY. I BELIEVE THEY ARE SUFFICIENT TO JUSTIFY A \$100,000 PAYMENT TO ME.

I MUST WARN OF CERTAIN RISKS TO MY SECURITY OF WHICH YOU MAY NOT BE AWARE. YOUR SERVICE HAS RECENTLY SUFFERED SOME SETBACKS. I WARN THAT MR. BORIS YUZHIN (LINE PR, SF), MR. SERGEY MOTORIN, (LINE PR, WASH.) AND MR. VALERIY MARTYNOV (LINE X, WASH.) HAVE BEEN RECRUITED BY OUR "SPECIAL SERVICES."

Boris Nikolayevich Yuzhin was a KGB Line PR officer assigned to the San Francisco residency under cover as a student from 1975 to 1976 and then as a TASS correspondent from 1978 to 1982. The FBI recruited Yuzhin to serve as an agent-in-place, and the FBI debriefed him. After returning to the Soviet Union, Yuzhin became the subject of an internal KGB investigation. Ames compromised Yuzhin to the KGB in June 1985 and by Hanssen in October 1985 as described above. Based in part on the information Hanssen gave the KGB, Yuzhin was arrested in December 1986, convicted of espionage, and sentenced to serve 15 years in prison. In 1992, he was released under a general grant of amnesty to political prisoners and subsequently immigrated to the United States.

Sergey Mikhailovich Motorin was a KGB Line PR officer assigned to the Soviet Embassy in Washington, DC, from June 1980 to January 1985. In January 1983, the FBI recruited Motorin to

serve as an agent-in-place, and the FBI debriefed him. Motorin returned to Moscow at the end of his tour of duty in January 1985. Ames and Hanssen compromised Motorin, like Martynov, to the KGB in June 1985 and October 1985, respectively. Based in part on the information Hanssen gave the KGB, Motorin was arrested in November or December 1985, tried and convicted on espionage charges during the period of October-November 1986, and executed in February 1987.

Valeriy Fedorovich Martynov was a KGB Line X officer assigned to the Soviet Embassy in Washington, DC, from October 1980 to November 1985. In April 1982, the FBI recruited Martynov to serve as an agent-in-place. He was debriefed jointly by the FBI and the CIA. Ames compromised Martynov to the KGB in June 1985 and by Hanssen in October 1985. Based in part on the information provided by Hanssen, the KGB directed Martynov to return to Moscow in November 1985, ostensibly to accompany KGB officer Vitaliy Yurchenko, who was returning to the Soviet Union after his August 1985 defection to the United States. Upon arriving in Moscow on 7 November 1985, Martynov was arrested. He was subsequently tried and convicted on espionage charges and then executed.

Hanssen proceeded to describe in detail a particular highly sensitive and classified information collection technique. This was on the existence of an FBI technical penetration of a particular Soviet establishment, as well as the specific location of the penetration device and the methods and technology utilized, which information was classified TOP SECRET and directly concerned communications intelligence.

In addition, "TO FURTHER SUPPORT MY BONA FIDES" he provided specific, closely held items of information regarding then-recent Soviet defectors. The information concerning the FBI's recruitment of Yuzhin, Motorin, and Martynov was classified at least at the SECRET level as was the defector information. The sensitive information collection technique was classified at the TOP SECRET level.

Hanssen added:

DETAILS REGARDING PAYMENT AND FUTURE CONTACT WILL BE SENT TO YOU PERSONALLY. . . . MY IDENTITY AND ACTUAL POSITION IN THE COMMUNITY MUST BE LEFT UNSTATED TO ENSURE MY SECURITY. I AM OPEN TO COMMO SUGGESTIONS BUT WANT NO SPECIALIZED TRADECRAFT. I WILL ADD 6, (YOU SUBTRACT 6) FROM STATED MONTHS, DAYS AND TIMES IN BOTH DIRECTIONS OF OUR FUTURE COMMUNICATIONS.

When Hanssen mailed this letter to the KGB he had recently been reassigned to New York City. However, FBI records show that on that particular day he was in Washington, DC, on administrative matters. The FBI information establishes Hanssen's ability to mail the letter from Washington, DC, rather than New York City where he was officially stationed.

True to his promise, Hanssen sent a package to Degtyar, which was received on 15 October 1985 at Degtyar's Alexandria residence. The package contained a large number of classified documents, including some original documents, of the US Intelligence Community. The next day at 8:35 am, FBI surveillance personnel observed Degtyar arriving at the Soviet Embassy carrying a large black canvas bag, which he did not typically carry.

On 8 November 1985, Degtyar and Cherkashin received a typed letter from Hanssen, which read in part as follows:

Thank you for the 50,000. I also appreciate your courage and perseverance in the face of generically reported bureaucratic obstacles. I would not have contacted you if it were not reported that you were held in esteem within your organization, an organization I have studied for years. I did expect some communication plan in your response. I viewed the postal delivery as a necessary risk and do not wish to trust again that channel with valuable material. I did this only because I had to so you would take my offer seriously, that there be no misunderstanding as to my long-term value, and to obtain appropriate security for our relationship from the start.

Hanssen then rejected the contact plans proposed by the KGB, and suggested a particular communications scheme based on “a microcomputer ‘bulletin board’” at a designated location, with “appropriate encryption.” Meanwhile, he wrote:

Let us use the same site again. Same timing. Same signals.” “B” proposed that the next dead drop occur on “September 9” which, according to the “6” coefficient that he established with the KGB in his first letter, actually meant that the dead drop operation would take place on March 3, 1986.

Hanssen also wrote:

As far as the funds are concerned, I have little need or utility for more than the 100,000. It merely provides a difficulty since I can not spend it, store it or invest it easily without tripping [sic] “drug money” warning bells. Perhaps some diamonds as security to my children and some good will so that when the time comes, you will accept by [sic] senior services as a guest lecturer. Eventually, I would appreciate an escape plan. (Nothing lasts forever.)

Referring to Yuzhin, Motorin, and Martynov, whom he had identified in his first letter as United States intelligence recruitments, Hanssen wrote:

I can not provide documentary substantiating evidence without arousing suspicion at this time. Never-the-less, it is from my own knowledge as a member of the community effort to capitalize on the information from which I speak. I have seen video tapes of debriefings and physically saw the last, though we were not introduced. The names were provided to me as part of my duties as one of the few who needed to know. You have some avenues of inquiry. Substantial funds were provided in excess of what could have been skimmed from their agents. The active one has always (in the past) used a concealment device – a bag with bank notes sewn in the base during home leaves.

In conclusion, Hanssen warned of a “new technique” used by NSA to collect against a specific Soviet target, which he described.

On 30 June 1986, Degtyar received another typed letter from Hanssen at his residence. The letter read in part as follows:

I apologize for the delay since our break in communications. I wanted to determine if there was any cause for concern over security. I have only seen one item which has given

me pause. When the FBI was first given access to Victor Petrovich Gundarev, they asked . . . if Gundarev knew Viktor Cherkashin. I thought this unusual. I had seen no report indicating that Viktor Cherkashin was handling an important agent, and here-to-fore he was looked at with the usual lethargy awarded Line Chiefs. The question came to mind, are they somehow able to monitor funds, ie., to know that Viktor Cherkashin received a large amount of money for an agent? I am unaware of any such ability, but I might not know that type of source reporting.

Viktor Gundarev was a KGB Line KR officer who defected to the United States on 14 February 1986. A classified FBI debriefing report, dated 4 March 1986, states that FBI debriefers showed Gundarev a photo of Cherkashin and asked if he knew Cherkashin.

Hanssen then informed the KGB that the United States knew of a particular technical vulnerability in Soviet satellite transmissions and was actively exploiting the vulnerability.

He concluded:

If you wish to continue our discussions, please have someone run an advertisement in the Washington Times during the week of 1/12/87 or 1/19/87, for sale, “Dodge Diplomat, 1971, needs engine work, \$1000.” Give a phone number and time-of-day in the advertisement where I can call. I will call and leave a phone number where a recorded message can be left for me in one hour. I will say, “Hello, my name is Ramon. I am calling about the car you offered for sale in the Times.” You will respond, “I’m sorry, but the man with the car is not here, can I get your number.” The number will be in Area Code 212. I will not specify that Area Code on the line.

Hanssen signed the letter “Ramon.”

According to the established “6” coefficient, the weeks the advertisement was actually to run were 6 July 1986, or 13 July 1986.

Before his PCS departure from the United States, Degtyar received an envelope at his residence. The envelope bore a handwritten address and a return address: “Ramon Garcia, 125 Main St, Falls Church VA.” It was postmarked from “NO VA MSC 22081” on 19 August 1986. MSC designates the Merrifield Service Center in Virginia. Inside the envelope was a handwritten note: “RECEIVED \$10,000. RAMON.”

On 11 September 1987, KGB Line PR officer Boris Malakhov received an envelope at his residence in Alexandria, Virginia. The envelope bore a handwritten address to "B.N. MALKOW" at the "NANCY" address—the "NANCY" address was the residence of Malakhov who replaced Degtyar as the Soviet Embassy press secretary. Hanssen was instructed to misspell Malakhov's name as "Malkow." The envelope had a handwritten return address of "R. GARCIA, 125 MAIN ST, ALEXANDRIA, VA," and was postmarked 8 September 1987.

Inside was the following typed letter:

Dear Friends:

No, I have decided. It must be on my original terms or not at all. I will not meet abroad or here. I will not maintain lists of sites or modified equipment. I will help you when I can, and in time we will develop methods of efficient communication. Unless a [sic] see an abort signal on our post from you by 3/16, I will mail my contact a valuable package timed to arrive on 3/18. I will await your signal and package to be in place before 1:00 pm on 3/22 or alternately the following three weeks, same day and time. If my terms are unacceptable then place no signals and withdraw my contact. Excellent work by him has ensured this channel is secure for now. My regards to him and to the professional way you have handled this matter.

Sincerely,

Ramon

According to the established "6" coefficient, the dates referred to in this letter were actually 10, 12, and 16 September.

On Monday, 14 September 1987, the KGB received in the mail a package of documents, including TOP SECRET National Security Council documents.

On 10 November 1987, Malakhov received a letter at his residence. The envelope bore a return address of "J. Baker" in "Chicago" and was postmarked on 7 November 1987. In the letter, Hanssen advised that Saturday for "AN" was not suitable, and he postponed the operation for two days, until Monday, 16 November. He advised that he had an urgent package for the KGB and asked

the KGB to place a signal confirming receipt of the letter. That same day, the KGB placed a signal at the "PARK" signal site. Thereafter, whenever Hanssen used the word "Chicago" in a return address, it was to signal that he intended for a deaddrop exchange to occur the following Monday.

On 4 February 1988, the KGB received a note from Hanssen at one of the new accommodation addresses given to Hanssen in the 23 November 1987 deaddrop. The address was the residence of a Soviet diplomatic official known to the FBI as a KGB co-optee located in Virginia. The note read simply "OK." It was in an envelope bearing a return address of "Jim Baker" in "Langley" and postmarked in Washington, DC, on 3 February 1988.

On 16 March 1988, the KGB received a second computer diskette from Hanssen at an accommodation address in Virginia. The envelope bore a return address of "Jim Baker" in "Chicago" and was postmarked in Washington, DC, on 15 March 1988.

The next day the KGB received another letter from Hanssen at an accommodation address in Virginia. The envelope bore a return address of "Jim Baker" in "Chicago" and was postmarked in Northern Virginia on 16 March 1988. In the letter, Hanssen instructed the KGB to use the "PARK/PRIME" deaddrop site until the KGB approved the other sites.

On 26 March 1988, the KGB received a third computer diskette from Hanssen at an accommodation address in Virginia. The envelope bore a return address of "Jim Baker" in "Chicago" and was postmarked in Washington, DC, on 24 March 1988. The KGB found no text on the diskette, which it referred to as "D-3."

The KGB received an envelope on 4 April 1988 from Hanssen at an accommodation address in Virginia. The envelope bore a return address of "Jim Baker" in "Alexandria" and was postmarked in Northern Virginia on 31 March 1988. In response to the KGB's indication that the diskette he sent was empty, Hanssen's note read "use 40 TRACK MODE, this letter is not a signal." The

term “use 40-track mode” refers to a technical process for reformatting a computer diskette in order to conceal data by putting the data onto specific tracks on the diskette. Unless a person uses the correct codes to decrypt such a diskette, the diskette would appear to be blank.

Two days later, on 6 April, the KGB received a package at an accommodation address in Virginia. The envelope bore a return address of “Jim Baker” in “Fairfax” and a postmark of “MSC NO VA” (Merrifield Service Center, Northern Virginia) on 5 April.

The package contained a fifth diskette (“D-5”). On the diskette, Hanssen provided what the KGB characterized as “everything” about a particular KGB officer and information about two specific Soviet FBI recruitments. Hanssen also explained why the KGB had been unable to read his diskettes. Hanssen also asked the KGB for diamonds. The KGB subsequently purchased several diamonds for use in the operation.

In addition, Hanssen provided information on KGB defector Victor Sheymov. He told the KGB that he could read the Viktor Sheymov file because a special project relating to Sheymov was about to begin.

At that time, Hanssen was reviewing the Sheymov file in preparation for his participation in upcoming Intelligence Community debriefings of Sheymov. Throughout the operation, Hanssen reported on Sheymov’s defection. Hanssen took particular interest in the Sheymov case and developed a personal friendship with Sheymov. In fact, Hanssen told FBI coworkers that he was considering an offer of lucrative employment by Sheymov after retirement in April 2001.

Victor Sheymov has been publicly identified as a former KGB Major, who worked in the 8th Chief Directorate of the KGB. At the time of his defection, he was responsible for coordinating KGB encrypted communications overseas. According to media reporting, the CIA smuggled Sheymov, his wife, and their 5-year-old daughter out of Moscow

on 16 May 1980. He now runs a computer security company called Invicta Networks.

On 24 May 1988, the KGB received a letter at an accommodation address in the District of Columbia. The envelope bore a return address of “Jim Baker” in “Chicago” and was postmarked in “MSC NO VA” on 17 May 1988. With the letter was Hanssen’s sixth diskette (“D-6”), which contained information about a number of matters. The diskette also contained information about a specific recent FBI Soviet recruitment operation.

The KGB received a letter on 15 July 1988 at an accommodation address in Virginia. The envelope bore a return address of “Chicago” and was postmarked “WDC 200” on 13 July 1988. The zip codes for Washington, DC, begin with “200.” The typed letter read as follows:

I found the site empty. Possibly I had the time wrong. I work from memory. My recollection was for you to fill before 1:00 a.m. I believe Viktor Degtyar was in the church driveway off Rt. 123, but I did not know how he would react to an approach. My schedule was tight to make this at all. Because of my work, I had to synchronize explanations and flights while not leaving a pattern of absence or travel that could later be correlated with communication times. This is difficult and expensive.

I will call the number you gave me on 2/24, 2/26 or 2/28 at 1:00 a.m., EDT. Please plan filled signals. Empty sites bother me. I like to know before I commit myself as I’m sure you do also. Let’s not use the original site so early at least until the seasons change. Some type of call-out signal to you when I have a package or when I can receive one would be useful. Also, please be specific about dates, e.g., 2/24. Scheduling is not simple for me because of frequent travel and wife. Any ambiguity multiplies the problems.

My security concerns may seem excessive. I believe experience has shown them to be necessary. I am much safer if you know little about me. Neither of us are children about these things. Over time, I can cut your losses rather than become one.

Ramon

P.S. Your “thank you” was deeply appreciated.

On 31 July 1988, the KGB received an envelope at an accommodation address in Virginia. The envelope bore a return address of Alexandria and contained a letter dated 29 July and Hanssen's seventh diskette ("D-7"), which contained information on technical surveillance systems, a new recruitment in New York City, illegal intelligence, and several other specific Soviet recruitment targets.

On 21 September 1988, the KGB received an envelope at an accommodation address in Virginia. The envelope bore a return address of "Chicago" and was postmarked "WDC" on September 20. The envelope contained Hanssen's eighth diskette ("D-8") and a note that read "At BOB." The diskette contained information about particular Soviet recruitment targets of the FBI.

On 1 December 1988, the KGB received a package at an accommodation address in Virginia. It bore a return address of "G. Robertson, Baker's Photo" and was postmarked "WDC" on 30 November 1988. The package contained a letter and his ninth diskette ("D-9") that contained information about a number of classified matters.

In October 1989, the KGB received two pieces of mail at an accommodation address in Virginia from Hanssen. The first piece of mail was received on 2 October. It was a letter bearing the return address "G. Robertson, 1408 Ingeborg Ct., McLean, VA" and postmarked "NO VA" on 28 September 1989. The letter reported that "The disk is clean. I tried all methods—completely demagnetized." The second piece of mail arrived on 17 October. It was an envelope bearing the return address "G. Robertson, 1101 Kingston Ct., Houston, TX" and postmarked "NO VA MSC 220" on 16 October 1989. The envelope contained Hanssen's sixteenth diskette ("D-16").

On 17 May 1990, the KGB received a letter and a diskette at an accommodation address in Virginia.

On 20 August 1990, the KGB received an envelope, containing Hanssen's twentieth diskette ("D-20"), at an accommodation address in Virginia. The

envelope bore the return address "J. Baker, Box 1101, Alexandria VA." The diskette contained classified information about several matters. Hanssen instructed the KGB to load the "FLO" deaddrop site on 3 September 1990.

On 12 December 1991, the KGB received an envelope at an accommodation address in Alexandria, Virginia. The envelope bore a handwritten return address of "J. Baker, Box 1101, Houston, TX" and was postmarked Washington, D.C. The envelope contained a handwritten note reading "—@ BOB on 6/22; T. DEVICE APPROVED 6/16, COMING SOON." Using the established "6" coefficient, the reference to "6/22" actually refers to 16 December. The reference to "T. DEVICE" related to information Hanssen had previously passed to the KGB regarding an FBI operation to plant a device in a technical surveillance operation against a Soviet person in the United States. Hanssen had reported this operation on 19 August 1991 to the KGB.

On 14 March 2000, Hanssen wrote a letter to the SVR, reading, in part, as follows:

. . . I have come about as close as I ever want to come to sacrificing myself to help you, and I get silence. I hate silence....Conclusion: One might propose that I am either insanely brave or quite insane. I'd answer neither. I'd say, insanely loyal. Take your pick. There is insanity in all the answers. I have, however, come as close to the edge as I can without being truly insane. My security concerns have proven reality-based. I'd say, pin your hopes on 'insanely loyal' and go for it. Only I can lose. I decided on this course when I was 14 years old. I'd read Philby's book. Now that is insane, eh! My only hesitations were my security concerns under uncertainty. I hate uncertainty. So far I have judged the edge correctly. Give me credit for that. Set the signal at my site any Tuesday evening. I will read your answer. Please, at least say goodbye. It's been a long time my dear friends, a long and lonely time.

Ramon Garcia

On 8 June 2000, Hanssen wrote another letter to the SVR that read, in part, as follows:

Dear Friends:

Administrative Issues:

Enclosed, once again, is my rudimentary cipher. Obviously it is weak in the manner I used it last—reusing key on multiple messages, but I wanted to give you a chance if you had lost the algorithm [sic]. Thank you for your note. It brought me great joy to see the signal at last. As you implied and I have said, we do need a better form of secure communication—faster. In this vein, I propose (without being attached to it) the following: One of the commercial products currently available is the Palm VII organizer. I have a Palm III, which is actually a fairly capable computer. The VII version comes with wireless internet capability built in. It can allow the rapid transmission of encrypted messages, which if used on an infrequent basis, could be quite effective in preventing confusions if the existence [sic] of the accounts could be appropriately hidden as well as the existence [sic] of the devices themselves. Such a device might even serve for rapid transmittal of substantial material in digital form. Your FAPSI could review what would be needed, its advisability, etc., obviously—particularly safe rules of use. While FAPSI may move with the rapidity of the Chinese army they can be quite effective, in juggernaut fashion, that is to say thorough. . . .

New topics:

If you are wise, you will reign [sic] in the GRU. They are causing no end of grief. But for the large number of double-agents they run, there would be almost no ability to cite activity warranting current foreign counterintelligence outlays. Of course the Gusev affair didn't help you any. If I'd had better communications I could have prevented that. I was aware of the fact that microphones had been detected at the State Department. (Such matters are why I need rapid communications. It can save you much grief.) Many such things are closely held, but that closeness fails when the need for action comes. Then the compartments grow of necessity. I had knowledge weeks before of the existence of devices, but not the country placing them. . . . I only found out the gruesome details too late to warn you through available means including the colored stick-pin call. (Which by the way I doubted would work because of your ominous silence.) Very frustrating. This is one reason I say 'you waste me' in the note. . . . The U.S. can be errantly likened to a powerfully built but retarded child, potentially dangerous, but young, immature and easily manipulated. But don't be fooled by that appearance. It is also one which can turn ingenious [sic] quickly, like an idiot savant, once convinced of a goal. The [] Japanese (to quote General Patten [sic] once again) learned this to their dismay. . . .

I will not be able to clear TOM on the first back-up date so don't be surprised if we default to that and you find this then. Just place yours again the following week, same protocol. I greatly appreciate your highly professional inclusion of old references to things known to you in messages resulting from the mail interaction to assure me that the channel remains unpirated. This is not lost on me.

On Swiss money laundering [sic], you and I both know it is possible but not simple. And we do both know that money is not really 'put away for you' except in some vague accounting sense. Never patronize at this level. It offends me, but then you are easily forgiven. But perhaps I shouldn't tease you. It just gets me in trouble. thank you again,

Ramon

On 17 November 2000, Hanssen wrote a letter to the KGB/SVR, reading, in part, as follows:

Dear Friends:

. . . together material for you now over a lengthy period. It is somewhat variable in import. Some were selected as being merely instructive rather than urgently important. I think such instructive Bear with me. It was I who sent the message trying to use TOM to communicate material to you. On reflection, I can understand why you did not respond. I see that I failed to furnish you sufficient information for you to recognize that the message you left for me in ELLIS did not go astray. You do this often (communicate such assurances through the mention of items like the old date offset we used), and believe me, it is not lost on me as a sign of professionalism. I say bear with me on this because you must realize I do not have a staff with whom to knock around all the potential difficulties. (For me breaks in communications are most difficult and stressful.) Recent changes in U.S. law now attach the death penalty to my help to you as you know, so I do take some risk. On the other hand, I know far better than most what minefields are laid and the risks. Generally speaking you overestimate the FBI's capacity to interdict you, but on the other hand, cocksure officers, (those with real guts and not as much knowledge as they think) can, as we say, step in an occasional cowpie. (Message to the translator: Got a good word for cowpie in Russian?? Clue, don't blindly walk behind cows.). . . . I have drawn insights often can be quite as valuable or even more valuable long-term because they are widely applicable rather than narrow. Others are of definite value immediately.

My position has been most frustrating. I knew Mr. Gusev was in eminent [sic] danger and had no effective way of communicating in time. I knew microphones of an unknown origin were detected even earlier and had no regular way of communicating even that. This needs to be rectified if I am to be as effective as I can be. No one answered my signal at Foxhall. Perhaps you occasionally give up on me. Giving up on me is a mistake. I have proven inveterately loyal and willing to take grave risks which even could cause my death, only remaining quiet in times of extreme uncertainty. So far my ship has successfully navigated the slings and arrows of outrageous fortune. I ask you to help me survive. . . .

On meeting out of the country, it simply is not practical for me. I must answer too many questions from family, friends, and government plus it is a cardinal sign of a spy. You have made it that way because of your policy. Policies are constraints, constraints breed patterns. Patterns are noticed. Meeting in this country is not really that hard to manage, but I am loath to do so not because it is risky but because it involves revealing my identity. That insulation has been my best protection against betrayal by someone like me working from whatever motivation, a Bloch or a Philby. (Bloch was such a shnook. . . . I almost hated protecting him, but then he was your friend, and there was your illegal I wanted to protect. If our guy sent to Paris had balls or brains both would have been dead meat. Fortunately for you he had neither. He was your good luck of the draw. He was the kind who progressed by always checking with those above and tying them to his mistakes. The French said, "Should we take them down?" He went all wet. He'd never made a decision before, why start then. It was that close. His kindred spirits promoted him. Things are the same the world over, eh?)

On funds transfers through Switzerland, I agree that Switzerland itself has no real security, but insulated by laundering on both the in and out sides, mine ultimately through say a corporation I control loaning mortgage money to me for which (re)payments are made.... It certainly could be done. Cash is hard to handle here because little business is ever really done in cash and repeated cash transactions into the banking system are more dangerous because of the difficulty in explaining them. That doesn't mean it isn't welcome enough to let that problem devolve on me. (We should all have such problems, eh?) How do you propose I get this money put away for me when I retire? (Come on; I can joke with you about it. I know money is not really put into an account at MOST Bank, and that you are speaking figuratively of an accounting notation at best to be made real at some uncertain future. We do the same. Want me to lecture in your 101 course in my old age? My college level Russian has sunk low through inattention all these years; I would be a novelty attraction, but I don't think a practical one except in extremis.) So good luck. Wish me luck. OK, on all sites detailed to date, but TOM's signal is unstable. See you in 'July' as you say constant conditions.

yours truly,

Ramon

Letters From the KGB/SVR

On 6 October 1999, Hanssen received the following letter from the SVR:

Dear friend:

Welcome! It's good to know you are here. Acknowledging your letter to V.K. we express our sincere joy on the occasion of resumption of contact with you. We firmly guarantee you for a necessary financial help. Note, please, that since our last contact a sum set aside for you has risen and presents now about 800.000 dollars. This time you will find in a package 50.000 dollars. Now it is up to you to give a secure explanation of it. As to communication plan, we may have need of some time to work out a secure and reliable one. This why we suggest to carry on the 13th of November at the same drop which you have proposed in your letter to V.K. We shall be ready to retrieve your package from DD since 20:00 to 21:00 hours on the 12th of November after we would read you [sic] signal (a vertical mark of white adhesive tape of 6 - 8 cm length) on the post closest to Wolfrap Creek of the "Foxstone Park" sign. We shall fill our package in and make up our signal (a horizontal mark of white adhesive tape). After you will clear the drop don't forget to remove our tape that will mean for us - exchange is over.

We propose a new place where you can put a signal for us when in need of an urgent DD operation. LOCATION: the closest to Whithaven [sic] Parkway wooden electricity utility pole at the south-west corner of T-shaped intersection of Foxhall Road and Whitehaven Parkway (map of Washington, DC, page 9, grid B11). At any working day put a white thumb tack (1 cm in diameter, colored sets are sold at CVS) into the Northern side of the pole at the height of about 1.2 yards. The tack must be seen from a car going down Foxhall Road. This will mean for us that we shall retrieve your package from the DD Foxstone Park at the evening of the nex [sic] week's Tuesday (when it's getting dark).

In case of a threatening situation of any kind put a yellow tack at the same place. This will mean that we shall refrain from any communication with you until further notice from your side (the white tack).

We also propose for your consideration a new DD site "Lewis". DD LOCATION: wooden podium in the amphitheatre of Long-branch Nature Center (map of N.Virginia, page 16, grid G8). The package should be put under the FAR-LEFT corner of the podium (when facing the podium). Enter [sic] Longbranch Nature Center at the sign from Carlin Springs Road (near 6th Road south) and after parking your car in the lot follow the sign "To Amphitheatre." LOCATION OF THE DD SIGNAL: a wooden electricity utility pole at the north-west corner of

the intersection of 3d Street and Carlin Springs Road nearq [sic] the Metrobus stop (the same map, grid F7). The signals are the same as in the "Foxstone Park" DD. The white adhesive tape should be placed on the NORTHERN side of the pole, so that it could be noticed fro [sic] a car moving along Carlin Springs Road in the southern direction from Route 50.

Please, let us know during the November operation of your opinion on the proposed places (the new signal and DD "Lewis"). We are intending to pass you a permanent communications plan using drops you know as well a new portion of money. For our part we are very interested to get from you any information about possible actions which may threaten us. Thank you. Good luck to you. Sincerely,

Your friends.

The initials "V.K." are those of a known SVR Line KR senior officer in Washington, DC.

On 31 July 2000, Hanssen received the following letter from the KGB/SVR:

Dear Ramon:

We are glad to use this possibility to thank You for Your striving for going on contact with us. We received Your message. The truth is that we expended a lot of efforts to decipher it. First of all we would like to emphasize that all well known events wich [sic] had taken place in this country and in our homeland had not affected our resources and we reaffirm our strong intentions to maintain and ensure safely our long-term cooperation with You.

We perceive Your actions as a manifestation of Your confidence in our service and from our part we assure You that we shall take all necessary measures to ensure Your personal security as much as possible. Just because proceeding from our golden rule – to ensure Your personal security in the first place – we have proposed to carry out our next exchange operation at the place which had been used in last august [sic]. We did not like to give You any occasion to charge us with an inadequate attention to problems of Your security. We are happy that, according to the version You have proposed in Your last letter, our suggestions about DD, known as "Ellis", coincided completely. However a situation around our colleagues [sic] at the end of passed [sic] year made us to refuse this operation at set day.

1. We thank You for information, which [sic] is of a great interest for us and highly evaluated in our service. We hope that during future exchanges we shall receive Your materials, which will deal with a [sic] work of IC, the FBI and CIA in the first place, against our representatives and officers. We do mean its human, electronic and

technical penetrations in our residencies here and in other countries. We are very interested in getting of the objective information on the work of a special group which serches [sic] "mole" in CIA and FBI. We need this information especially to take necessary additional steps to ensure Your personal security....

2. Before stating a communication plan that we propose for a next future, we would like to precise [sic] a following problem. Do You have any possibility to meet our colleagues [sic] or to undertake the exchange ops in other countries? If yes, what are these countries? Until we receive Your answer at this [sic] questions and set up a new communication plan, we propose to use for the exchange ops DD according to the following schedule:
 - = DD "LEWIS" on 27 of may 2001 (with a coefficient it will mean on 21 of november 2000). We draw Your attention on the fact that we used a former coefficient -6 (sender adds, addressee subtracts). A time will be shown at real sense. We will be ready to withdraw Your package beginning by 8 PM on 27 may 2001 after we shall read Your signal. After that we put DD our package for You. Remove Your signal and place our signal by 9 PM of the same day. After that You will withdraw our package and remove our signal. That will mean an exchange operation is over. We shall check signal site (i.e., its absence) the next day (28 of May) till 9 PM. If by this time a signal had not been removed we shall withdraw our package and shall put it in for You repeatedly dates with DD "ELLIS"— in each seven days after 28 May till 19 of June 2001 (i.e., 13 of December 2000).
 - = We propose to carry out our next operation on 16 of october 2001 (i.e., 10 of April) at the DD "LINDA" in "Round Tree park" (if this place suits for Your [sic] we would like to receive Your oppinion [sic] about that during exchange in may). A time of operation from 8 pm to 9 pm, signals and schedule of alternate dates are the same. In the course of exchange ops we shall pass to You descriptions of new DD and SS that You can check them before. You will find with this letter descriptions of two new DD "LINDA" and "TOM". Hope to have Your opinion about them. In case of break off in our contacts we propose to use DD "ELLIS", that you indicated in your first message. Your note about a second bridge across the street from the 'F' sign, as back up, is approved. We propose to use "ELLIS" once a year on 12 August (i.e., with coeff. it will be 18 February) at the same time as it was in August 1999. On that day we can carry out a full exchange operation— You will enload your package and put a signal, we shall withdraw it, load our package and put our signal. You will remove our package and put your signal. Alternate dates – in seven days 'til next month.

- = As it appears from your message, you continue to use post channel as a means of communication with us. You know very well our negative attitude toward this method. However if you send by post a short note where date (i.e., with coefficient), time and name of DD for urgent exchange are mentioned, you could do it by using address you had used in September (i.e., with coeff.) putting in a sealed envelope for V.K. In future it is inexpedient to use a V.K. name as a sender. It will be better to choose any well known name in this country as you did it before.
- 3. We shall continue work up [sic] new variants of exchanging messages including PC disks. Of course we shall submit them to your approval in advance. If you use a PC disk for next time, please give us key numbers and program you have used.
- 4. We would like to tell you that an insignificant number of persons know about you, your information and our relationship.
- 5. We assess as very risky to transfer money in Zurich because now it is impossible to hide its origin...

Newspaper Ads/Telephone Calls

In response to Hanssen's request in the 30 June 1986 letter, the following advertisement appeared in the *The Washington Times* from 14 July 1986, to 18 July 1986:

DODGE - '71, DIPLOMAT, NEEDS ENGINE WORK, \$1000. Phone (703) 451-9780 (CALL NEXT Mon., Wed., Fri. 1 p.m.).

The number 703/451-9780 at that time belonged to a public telephone located in the vicinity of the Old Keene Mill Shopping Center in Fairfax County, Virginia. On Monday, 21 July 1986, Hanssen called that number and gave the number 628-8047. Aleksandr Kirillovich Fefelov, a KGB officer assigned to the Soviet Embassy in Washington, DC, took the call.

One hour later, Fefelov telephoned 212/628-8047 and told Hanssen that the KGB had loaded the "PARK" deaddrop site. The KGB mistakenly placed the package under the wrong corner of the wooden footbridge at the "PARK" site.

On 7 August 1986, Degtyar received a letter from Hanssen stating that he had not found the package at the deaddrop site and indicating that he would phone 703/451-9780 on 18, 20, or 22 August. The KGB then retrieved its package from the "PARK" deaddrop site.

On Monday, 18 August 1986, Hanssen telephoned 703/451-9780 and spoke with Fefelov.³ The latter portion of the conversation was recorded as follows: ([UI] = unintelligible)

Hanssen: *Tomorrow morning?*

FEFELOV: *Uh, yeah, and the car is still available for you and as we have agreed last time, I prepared all the papers and I left them on the same table. You didn't find them because I put them in another corner of the table.*

Hanssen: *I see..*

FEFELOV: *You shouldn't worry, everything is okay. The papers are with me now.*

Hanssen: *Good.*

FEFELOV: *I believe under these circumstances, mmmm, it's not necessary to make any changes concerning the place and the time. Our company is reliable, and we are ready to give you a substantial discount which will be enclosed in the papers. Now, about the date of our meeting. I suggest that our meeting will be, will take place without delay on February thirteenth, one three, one p.m. Okay? February thirteenth.*

Hanssen: [UI] *February second?*

FEFELOV: *Thirteenth. One three.*

Hanssen: *One three.*

FEFELOV: *Yes. Thirteenth. One p.m.*

Hanssen: *Let me see if I can do that. Hold on.*

FEFELOV: *Okay. Yeah.*

[pause]

Hanssen: [whispering] [UI]

FEFELOV: *Hello? Okay.*

[pause]

Hanssen: [whispering] *Six . . . Six . . .*

[pause]

Hanssen: *That should be fine.*

FEFELOV: *Okay. We will confirm you, that the papers are waiting for you with the same horizontal tape in the same place as we did it at the first time.*

Hanssen: *Very good.*

FEFELOV: *You see. After you receive the papers, you will send the letter confirming it and signing it, as usual. Okay?*

Hanssen: *Excellent.*

FEFELOV: *I hope you remember the address. Is . . . if everything is okay?*

Hanssen: *I believe it should be fine and thank you very much.*

FEFELOV: *Heh-heh. Not at all. Not at all. Nice job. For both of us. Uh, have a nice evening, sir.*

Hanssen: *Do svidaniya.*

FEFELOV: *Bye-bye.*

According to the established “6” coefficient, the operation discussed in this conversation was actually scheduled to occur on 19 August 1986 at 7:00 a.m.

Deaddrops

“PARK/PRIME”

In 1985, when Hanssen volunteered to the KGB, he lived on Whitecedar Court in Vienna, Virginia. The first deaddrop site selected by Hanssen was Nottoway Park, which was less than a five-minute walk from his home. Between 1985 and 1989, the Nottoway Park site was used for deaddrops so frequently—17 times—that it was designated by the KGB as the “PARK/PRIME” deaddrop site.

Degtyar received a typed message by mail delivered to his Alexandria residence. The envelope had a handwritten address and postmarked “New York, NY” on 24 October 1985.

The message included the following text:

DROP LOCATION

Please leave your package for me under the corner (nearest the street) of the wooden foot bridge located just west of the entrance to Nottoway Park. (ADC Northern Virginia Street Map, #14, D3)

PACKAGE PREPARATION

Use a green or brown plastic trash bag and trash to cover a waterproofed package.⁴

SIGNAL LOCATION

Signal site will be the pictorial “pedestrian-crossing” signpost just west of the main Nottoway Park entrance on Old Courthouse Road. (The sign is the one nearest the bridge just mentioned.)

SIGNALS

My signal to you: One vertical mark of white adhesive tape meaning I am ready to receive your package. Your signal to me: One horizontal mark of white adhesive tape meaning drop filled. My signal to you: One vertical mark of white adhesive tape meaning I have received your package. (Remove old tape before leaving signal.)

The message established a date and times for the signals and drops and concluded, “I will acknowledge amount with my next package.”

The KGB designated this deaddrop site by the codename “PARK.” It is located in Fairfax County, Virginia.

On Saturday, 2 November 1985, the KGB loaded the “PARK” deaddrop site with \$50,000 in cash and a message proposing procedures for future contacts with Hanssen.

On 3 March 1986, the KGB loaded the “PARK” dead drop site, but Hanssen did not appear; therefore, the KGB removed its package from the deaddrop site the same day.

As a result of the conversation between Fefelov and Hanssen on 18 August 1986, the KGB loaded the “PARK” deaddrop site with \$10,000 in cash. They also included proposals for two additional deaddrop sites to be used by Hanssen and the KGB, a new accommodation address codenamed “NANCY,” and emergency communications plans

for Hanssen to personally contact KGB personnel in Vienna, Austria. Hanssen subsequently cleared the deaddrop.

On Tuesday, 15 September 1987, the KGB loaded the “PARK” deaddrop site with \$10,000 cash. The KGB also proposed two additional deaddrop sites, one codenamed “AN” located in Ellanor C. Lawrence Park in western Fairfax County, Virginia, and another codenamed “DEN” at a different location farther away. The KGB proposed that Hanssen load the deaddrop at “PARK” or “AN” on 26 September 1987, and that the KGB respond by loading “DEN.”

The next day the KGB determined that Hanssen had cleared the “PARK” deaddrop and removed the signal.

On 26 September 1987, the KGB recovered from the “PARK” deaddrop site a package from Hanssen. The package contained a handwritten letter reading as follows:

My Friends:

Thank you for the \$10,000. I am not a young man, and the commitments on my time prevent using distant drops such as you suggest. I know in this I am moving you out of your set modes of doing business, but my experience tells me the [sic] we can be actually more secure in easier modes.

Hanssen then suggested an exchange procedure involving a parked car instead of a deaddrop site and a related communications procedure, but stated:

“If you cannot do this I will clear this once ‘AN’ on your scheduled date (rather than the other).” He then asked the KGB to “Find a comfortable Vienna VA signal site to call me to an exchange any following Monday.” He closed the letter, “Good luck with your work”, and signed it “Ramon.”

The package also contained a document, which the KGB described as having the title, which roughly translates into English, as “National Intelligence Program for 87.”

In response to Hanssen’s request, the KGB proposed a signal site in Vienna, Virginia, on the

post of a stop sign on the shoulder of Courthouse Road near its junction with Locust Street. This signal site was referred to as “V.”

On Monday, 23 November 1987, Hanssen and the KGB carried out an exchange operation at “PARK.” The package from Hanssen contained several items. One was a cable-type report about a meeting in October 1987 with a valuable source, whom the KGB referred to as “M.” Another was a report about a recent FBI/CIA meeting with a Soviet intelligence officer who was an FBI/CIA recruitment target. The last items were a survey of information provided by Vitaliy Yurchenko and an official technical document describing COINS-II. In 1987, COINS-II was the then-current version of the US Intelligence Community’s “Community On-line Intelligence System,” which constituted a classified Community-wide Intranet.

The KGB package contained \$20,000 cash and a letter conveying “regards” from the KGB Director and advising that \$100,000 had been deposited in a bank at 6- to 7-percent interest. The letter also asked Hanssen for a variety of specific, classified information. The KGB gave Hanssen two new accommodation addresses and asked him to propose new deaddrop sites.

On Monday, 8 February 1988, Hanssen and the KGB carried out another exchange operation at the “PARK,” which the KGB had now renamed “PRIME.”

The package to the KGB contained a typed, unsigned letter. In the letter, Hanssen acknowledged receipt of \$20,000 and identified two additional drop sites.

He then went on to provide detailed information concerning a recruited KGB officer who had secretly defected to the United States. He advised the KGB that he had arranged time to review the defector’s file. “A full report will follow as soon as possible.”

He also provided the identity, by KGB codename and recent specific assignment, of a KGB agent who was currently operating as an illegal in a particular

US city and who had been recruited by the FBI to serve as a double agent. He then disclosed to the KGB a particular limitation of NSA's ability to read certain Soviet communications.

Enclosed with the letter was the first computer diskette that Hanssen passed to the KGB. Also in the package were classified documents.

The package from the KGB contained \$25,000 cash and a letter conveying thanks of the KGB Chairman, Vladimir Kryuchkov, for the information about the valuable source "M." The KGB also asked Hanssen for more information about "M" and the "agent network" in New York City and about a particular KGB officer.

On the next day, 9 February 1988, the KGB observed that the signal at "PARK/PRIME" had been removed, indicating that Hanssen had cleared the drop.

On Monday, 21 March 1988, the KGB observed a signal from Hanssen at "PARK/PRIME," but was unable to check the deaddrop because strangers were present in the park.

One week later, on Monday, 28 March 1988, Hanssen and the KGB carried out an exchange operation at "PARK/PRIME." The package to the KGB contained Hanssen's fourth computer diskette ("D-4"). It also included a TOP SECRET document entitled "The FBI's Double Agent Program," which contained a detailed evaluation of FBI double agent operations, including joint operations with other US intelligence agencies, and a document that the KGB described as a Director of Central Intelligence (DCI) document entitled "Stealth Orientation."

The package from the KGB included \$25,000 cash and a letter explaining why the KGB had not been able to check the "PARK/PRIME" deaddrop site on 21 March. In the letter, the KGB also advised it had been unable to read the diskettes Hanssen had passed to the KGB. The KGB asked Hanssen for information about codes and cryptograms, intelligence support for the Strategic Defense Initiative, submarines, and other classified material.

The next day, the KGB observed that Hanssen had removed the signal from the "PARK/PRIME" site, indicating he had removed the package.

On Monday, 30 May 1988, a KGB officer arrived at "PARK/PRIME" at 9:03 p.m., three minutes after the end of the prearranged deaddrop exchange period. The KGB officer saw a man who apparently removed the signal, got into his car, and drove away.

Hanssen and the KGB carried out an exchange operation on Monday, 18 July 1988, at "PARK/PRIME." The package from Hanssen contained more than 530 pages of material, including:

- A CIA document concerning intelligence analysis of the effectiveness of Soviet intelligence collection efforts against certain US nuclear weapons capabilities, which analysis directly concerned early warning systems and other means of defense or retaliation against large-scale attack. The document was dated approximately November 1987 and classified TOP SECRET with the caveats NOFORN NOCONTRACT ORCON.
- A DCI document entitled "Compendium of Future Intelligence Requirements: Volume II," dated September 1987, prepared by the Staff of the Intelligence Producers Council, and classified TOP SECRET/SCI with the caveat NOFORN. It contained a comprehensive listing of specific current intelligence information, including information about military capabilities and preparedness, sought by the United States regarding the Soviet Union and other nations.
- A CIA Counterintelligence Staff Study entitled "The Soviet Counterintelligence Offensive: KGB Recruitment Operations Against CIA," dated March 1988 and classified SECRET with the caveats NOFORN NOCONTRACT ORCON. This document contains the following preface: Warning Notice Intelligence Sources or Methods Involved (WNINTEL) National Security Unauthorized Disclosure Information Subject to Criminal Sanctions and

also specifically defining “NOFORN” as “Not Releasable to Foreign Nationals.”

- A TOP SECRET comprehensive historical FBI review of allegations from recruitments and defectors over a period of years that the Soviet intelligence services had penetrated the US Intelligence Community. It identified Soviet recruitments and defectors with specificity and describes particular information they provided. It contained the following warning:

IN VIEW OF THE EXTREME SENSITIVITY OF THIS DOCUMENT, THE UTMOST CAUTION MUST BE EXERCISED IN ITS HANDLING. THE CONTENTS INCLUDE A COMPREHENSIVE REVIEW OF SENSITIVE SOURCE ALLEGATIONS AND INVESTIGATIONS OF PENETRATION OF THE FBI BY THE SOVIET INTELLIGENCE SERVICES, THE DISCLOSURE OF WHICH WOULD COMPROMISE HIGHLY SENSITIVE COUNTERINTELLIGENCE OPERATIONS AND METHODS. ACCESS SHOULD BE LIMITED TO A STRICT NEED-TO-KNOW BASIS.

The package from the KGB contained \$25,000 cash and a letter asking for information about surveillance systems, the agent network in New York City, illegal intelligence, and several specific FBI recruitment operations. The KGB proposed two new deaddrop and related signal sites. One, named “BOB,” was under a footbridge in Idylwood Park between Vienna and Falls Church, Virginia. The other, named “CHARLIE,” was under a footbridge in Eakin Community Park, south of Vienna. For these deaddrop sites, the KGB instructed Hanssen to load the deaddrops by 9:00 p.m. on the designated day; the KGB would clear it by 10:00 p.m. and load it with a package, which Hanssen was to clear after 10:00 p.m.

The KGB marked the “V” signal site on Courthouse Road in Vienna on 24 March 1989 indicating that Hanssen should pick up a package at “PARK/PRIME” the following Monday. On Monday, 27 March 1989, the KGB loaded the dead drop with the MASINT document, for return to Hanssen but Hanssen did not clear the drop.

“AN”

On Sunday, 15 November 1987, the KGB loaded the “AN” deaddrop site with a package. It was not cleared by Hanssen and the KGB retrieved the package on 17 November.

On Thursday, 19 November 1987, the KGB received a handwritten letter from Hanssen. The envelope bore a return address of “G. Robertson” in “Houston” and was postmarked on 17 November 1987. The letter read as follows:

Unable to locate AN based on your description at night. Recognize that I am dressed in business suit and can not slog around in inch deep mud. I suggest we use once again original site. I will place my urgent material there at next AN times. Replace it with your package. I will select some few sites good for me and pass them to you. Please give new constant conditions of recontact as address to write. Will not put substantive material through it. Only instructions as usual format.

Ramon

“BOB”

On Monday, 26 September 1988, Hanssen and the KGB carried out an exchange operation at “BOB.” The package from Hanssen contained approximately 300 pages of material. Among the material was an FBI memo about a particular individual believed at the time to be a KGB Line KR officer in New York City, information on technical means of Soviet intelligence, a transcript of a Counterintelligence Group meeting, and information on several other matters.

The KGB package contained a diamond valued at \$24,720 and a letter advising Hanssen that \$50,000 had been deposited in his account. The letter also expressed gratitude to Hanssen from the KGB Chairman (Vladimir A. Kryuchov). The letter also discussed communications procedures, security measures, a personal meeting, and passports. It also asked Hanssen to provide information about classified technical operations in the Soviet Union, agent network details, allies’ sources, FBI programs, past cases, and a certain missile technology.

On Tuesday, 31 January 1989, the KGB observed an emergency call-out signal at a signal site that it had issued to Hanssen located at the intersection of Q Street and Connecticut Avenue, NW, Washington, D.C. By prearrangement, the KGB immediately unloaded a package from Hanssen at "BOB." The package contained a cable, with a note reading:

"Send to the Center right away. This might be useful."

Also in the package was Hanssen's eleventh diskette ("D-11"), which contained comments on the cable, as well as information on several specific individuals about whom the KGB had asked for information.

Espionage does not take a holiday. When every one else was enjoying Christmas Day with their families, Hanssen and the KGB were conducting an exchange operation at "BOB" on Monday, 25 December 1989. After a call-out signal from Hanssen, the KGB retrieved a package from Hanssen, which contained his seventeenth diskette ("D-17") and several documents, including a DCI National Intelligence Estimate entitled "The Soviet System in Crisis: Prospects for the Next Two Years" and dated November 1989. This document was classified SECRET, bore the caveats NOFORN NOCONTRACT WNINTEL, and contained the notice "Unauthorized Disclosure Subject to Criminal Sanctions." He also provided additional documents on the highly sensitive technical penetration of the Soviet establishment.

The diskette contained a message in which Hanssen complimented the KGB's efficient actions and provided current information about several ongoing FBI recruitment operations against Soviet intelligence officers; three new highly protected FBI sources within the KGB and other Soviet entities; and four defectors. He also provided updated information on the Bloch-Gikman matter.

The KGB package contained \$38,000 cash as payment for the period 16-23 October period in addition to compensation for the two returned diamonds and two KGB diskettes. The diskettes contained Christmas greetings from the KGB,

discussed communications plans, and asked Hanssen for specific information about a variety of classified technical operations.

On Monday, 16 December 1991, Hanssen and the KGB carried out an exchange operation at "BOB." The package to the KGB contained several documents, including:

- (A) A DCI Counterintelligence Center research paper entitled "The KGB's First Chief Directorate: Structure, Functions, and Methods," dated November 1990. The document was classified SECRET with the caveats NOFORN NOCONTRACT ORCON. It also bore the following notices: WARNING NOTICE This document should be disseminated only to persons having both the requisite clearances and a need to have access to its contents for performance of their duties. No further distribution or reproduction is authorized without the approval of the Associate Deputy Director for Operations for Counterintelligence, CIA and National Security Unauthorized Disclosure Information Subject to Criminal Sanctions.
- (B) A volume of the DCI Intelligence FY 1992 Congressional Budget Justification Volume X that detailed the programs and resource needs of the FBI's Foreign Counterintelligence Program. The document was classified SECRET with the caveats NOFORN NOCONTRACT ORCON and the warning "Unauthorized Disclosure Subject to Criminal Sanctions."

The package from Hanssen also contained his twenty-sixth diskette ("D-26") in which he expressed embarrassment over the pages missing from his earlier package. He advised that he had been promoted to a position of increase in salary and authority [which] moved him temporarily out of direct responsibility, but a new mission for my new group has not been fully defined" and that "I hope to adjust to thatAs General Patton said . . . 'let's get this over with so we can go kick the

[] out of the [] Japanese.” He noted that a new mission for his new group had not yet been defined, and he quoted a particular remark by General Patton about the Japanese.

He later quoted the same reference to Japanese in the letter he wrote to the SVR on 8 June 2000. At that time, Hanssen was preparing to assume new duties as Chief of the new National Security Threat List Unit at FBI Headquarters, where he focused the Unit’s counterintelligence efforts on economic espionage. This new assignment resulted in an increase in salary (from GS-14 to GS-15) and authority (Unit Chief). Several FBI employees recall that Hanssen frequently quoted General Patton, and one employee who worked closely with Hanssen specifically remembers Hanssen once using the above-mentioned Patton quote in a discussion with him.

Hanssen discussed communications plans and provided information about various classified technical and operational matters, including again information that the US Intelligence Community was obtaining especially sensitive material from the communications of a specific foreign country. He also proposed a new communications system, in which he would set up an office at a location in town not subject to electronic surveillance, where he and the KGB could communicate directly using a computer that would be specially equipped with certain advanced technology.

The package from the KGB contained \$12,000 cash and a KGB diskette discussing communications plans and asking for specific information about various classified matters.

In one message to “B” the KGB warned him to “Examine from the point of security Your practice of copying materials.”

“CHARLIE”

On Monday, 26 December 1988, Hanssen and the KGB carried out an exchange operation at “CHARLIE.”

The package from Hanssen contained his tenth diskette (“D-10”) and approximately 356 pages of material. On the diskette, Hanssen provided additional classified information.

He also provided six recent National HUMINT Collection Plan (NHCP) documents and a document whose title the KGB noted as “Soviet Armed Forces and Capabilities for Conducting Strategic Nuclear War Until the End of the 1990s.” In addition, he passed a TOP SECRET document on the fact that the United States was targeting a particular category of Soviet communications.

The package from the KGB contained \$10,000 cash, a second diamond valued at \$17,748, and a message in which the KGB asked Hanssen for additional specific information about a wide variety of classified technical and recruitment matters.

The next day, the KGB observed that the signal at the “CHARLIE” site had been removed, indicating Hanssen had removed the KGB’s package.

The “CHARLIE” site was used again after Hanssen marked on Thursday, 16 March 1989, a call-out signal site that the KGB has issued to him, located at the Taft Bridge in Northwest Washington, DC.

On Monday, 20 March 1989, Hanssen and the KGB carried out an exchange operation at “CHARLIE.” Hanssen passed two packages to the KGB.

One contained a TOP SECRET/SCI document entitled “DCI Guidance for the National MASINT Intelligence Program (FY 1991-FY 2000),” prepared by the Measurement and Signature Intelligence (MASINT) Committee and dated November 1988. The document bears the caveats NOFORN and NOCONTRACT and contains the following preface: Warning Notice Intelligence Sources or Methods Involved (WNINTEL) NATIONAL SECURITY INFORMATION Unauthorized Disclosure Subject to Criminal Sanctions.

According to its Introduction, this document contains the MASINT Committee’s

recommendations to the DCI for the collection, processing, and reporting of MASINT and represents the Intelligence Community's consensus on specific MASINT objectives and studies leading to needed capabilities. Its contents are highly specific and technical. In passing this document to the KGB, Hanssen requested that it be returned.

The second package from Hanssen contained his twelfth computer diskette ("D-12") and approximately 539 pages of materials, including classified information on a variety of matters.

The KGB package contained \$18,000 cash and a third diamond, valued at \$11,700. It also contained a letter that confirmed the KGB had received Hanssen's packages on 26 December and 31 January, discussed a personal meeting, requested new deaddrop sites, and asked how to increase operational security. The KGB also asked Hanssen about his security precautions for the diamonds. (Hanssen told the KGB that he would say the diamonds came from his grandmother.) The KGB also asked for information about a wide variety of technical and operational subjects. The KGB thanked Hanssen for the information he provided on 31 January, and asked him "for everything else that's possible."

On Tuesday, 21 March 1989, the KGB observed that the signal at "CHARLIE" had been removed, indicating that Hanssen had removed the KGB's package.

On Monday, 7 August 1989, after two call-out signals from Hanssen, he and the KGB carried out an exchange operation at "CHARLIE."

In the package from Hanssen were five rolls of film containing highly-restricted TOP SECRET/SCI analysis dated May 1987 of the foreign threat to a specific and named highly-compartmented US Government program to ensure the continuity of government in the event of a Soviet nuclear attack, which analysis directly concerned means of defense or retaliation against large-scale nuclear attack and other elements of defense strategy. Also in the package was his fourteenth diskette ("D-14"), which contained information from the Bloch-Gikman file and several FBI recruitment attempts.

Felix Bloch had been identified as an associate of Austria-based known Soviet illegal Reino Gikman on the basis of a telephone call between them on 27 April 1989. One day later, the FBI opened a classified investigation of Bloch, who at the time was assigned to the State Department in Washington, DC. Meetings between Bloch and Gikman were observed in Paris on 14 May 1989 and in Brussels on 28 May 1989.

In early June 1989, after Hanssen had compromised the Bloch investigation, Gikman suddenly left for Moscow. Early on the morning of 22 June 1989, Bloch received a telephone call at his home in Washington, DC, from a man identifying himself as Ferdinand Paul. According to a recording of that call, Ferdinand Paul told Bloch that he was calling "in behalf of Pierre" who "cannot see you in the near future" because "he is sick" and that "a contagious disease is suspected." (Bloch knew Gikman as Pierre.) Paul then told Bloch, "I am worried about you. You have to take care of yourself."

Having concluded that this call alerted Bloch that his association with Gikman had been compromised, the FBI interviewed Bloch on 22 and 23 June 1989. Bloch denied he had engaged in espionage and ultimately declined to answer any further questions. The FBI was unable further to develop its investigation of Bloch.

Hanssen approved a new deaddrop site that the KGB had proposed, codenamed "DORIS," located under a footbridge in Canterbury Park in Springfield, Virginia.

The KGB's package to Hanssen contained \$30,000 cash and a letter promising to compensate him for the returned diamonds. The KGB rejected his suggestions for an account in Switzerland. The KGB discussed communications plans, and proposed a new deaddrop site, codenamed "ELLIS," under a footbridge over Wolftrap Creek near Creek Crossing Road at Foxstone Park near Vienna, Virginia, with a signal site on the "Foxstone Park" sign.

The next day, the KGB observed that the signal associated with the “CHARLIE” deaddrop site had been removed, indicating that “B” had retrieved the KGB’s package.

“CHARLIE” was again used on Monday, 5 March 1990, after a call-out signal from Hanssen. Hanssen’s package contained his eighteenth diskette (“D-18”). It contained classified information on a wide variety of topics, including a KGB officer in the Soviet Embassy, a Soviet illegal, and two KGB defectors, who were all serving as FBI-CIA sources; communications intelligence operations; and the identification of a particular named NSA employee and the sensitive office in which the employee worked. The package also contained a 120-page document whose title, according to KGB records, was “Soviet Armed Forces and Strategic Nuclear Capabilities for the 1990s,” dated February 1990.

The package from the KGB contained \$40,000 cash and a KGB diskette. The diskette discussed communications plans and asked Hanssen to provide information on a wide range of classified technical, operational, and recruitment matters. The KGB also asked Hanssen what the Soviets could use of the certain highly classified and sensitive program information he had previously disclosed.

On Saturday, 2 February 1991, in response to an emergency call-out signal from Hanssen, the KGB retrieved a package from “CHARLIE.” The package contained Hanssen’s twenty-first diskette (“D-21”), which included a letter in which “B” acknowledged receipt of the \$40,000, which he characterized as “too generous.”

He disclosed to the KGB that the FBI’s chief of counterintelligence in the New York Field Office had told him that the FBI had recruited a specific number of sources at a particular Soviet establishment. Hanssen also advised that he would be ready for an operation on 18 February 1991.

In exchange, the KGB left a package for Hanssen but he did not pick it up and the KGB later retrieved it.

The KGB reloaded “CHARLIE” on Monday, 18 February, with the package Hanssen did not retrieve previously. It contained \$10,000 cash and a KGB diskette. The diskette established two new deaddrop sites, one of which was codenamed “GRACE” and located under a footbridge in Rock Creek Park in Washington, DC. It also asked Hanssen to provide specific classified technical and operational information, and instructed that the next contact would be at the “DORIS” site.

“DORIS”

On Monday, 25 September 1989, Hanssen and the KGB carried out an exchange operation at “DORIS.” The package to the KGB contained approximately 80 pages of material, including part of a document concerning a highly sensitive United States technical penetration of a particular Soviet establishment classified at the TOP SECRET/SCI level. In passing this document, Hanssen compromised a program of enormous value, expense, and importance to the United States. In addition, another document concerned a technical operation against a specific foreign target classified TOP SECRET and directly concerned communications intelligence. Also in the package was his fifteenth diskette (“D-15”), containing additional classified information. The package from the KGB contained \$30,000 cash, a letter, and, for the first time from the KGB, a computer diskette.

The “DORIS” drop was not used again until Monday, 7 May 1990, after a call-out signal from Hanssen. The package from Hanssen contained his nineteenth diskette (“D-19”) and approximately 232 pages of material, including another document on the tightly compartmented classified program to ensure the continuity of the US Government in the event of a Soviet nuclear attack, which Hanssen had informed the KGB in a document passed to them on 7 August 1989.

Hanssen also gave the KGB permission to use the certain highly classified and sensitive program information he had previously disclosed. Hanssen also advised that because of a promotion he

would be traveling for one year, and he discussed communications plans and a method of renewing contact. [NOTE: In May 1990, Hanssen was reassigned from the Soviet Analytical Unit in the Intelligence Division to the Inspection Division at FBI Headquarters. An Inspection Division assignment is a typical feature of an FBI supervisory agent's career path and requires frequent travel to FBI field offices for inspections. While serving in this assignment, Hanssen traveled frequently from June 1990 through June 1991 to conduct inspections in various FBI offices.]

The KGB package to Hanssen contained \$35,000 cash and a KGB diskette. The diskette contained communications plans and identified a new deaddrop site, codenamed "FLO," located under a footbridge in Lewinsville Park near the intersection of Warner Avenue and Westbury Road in McLean, Virginia, and a nearby signal site. The diskette also contained specific requests for information, including operational leads and materials on recruitments of Soviets. It read, in part, as follows:

Dear Friend:

. . . . We attach some information requests which we ask Your kind assistance for. We are very cautious about using Your info and materials so that none of our actions in no way causes [sic] no harm to Your security. With this on our mind we are asking that sensitive materials and information (especially hot and demanding some actions) be accompanied by some sort of Your comments or some guidance on how we may or may not use it with regard to Your security. We wish You good luck and enclose \$35,000. Thank you.

Sincerely,

Your friends.

In response to a call-out signal from Hanssen, he and the KGB executed an exchange operation on Monday, 15 April 1991 at "DORIS." The package to the KGB contained his twenty-second diskette ("D-22") in which he confirmed receipt of cash. Hanssen also provided classified FBI material about a specific recruitment operation about which the KGB had previously asked. The package from the KGB contained \$10,000 and a KGB diskette that read, in part, as follows:

Dear Friend:

Time is flying. As a poet said: "What's our life, If full of care You have no time To stop and stare?" You've managed to slow down the speed of Your running life to send us a message. And we appreciate it. We hope You're O'K and Your family is fine too. We are sure You're doing great at Your job. As before, we'll keep staying alert to respond to any call from You whenever You need it. We acknowledge receiving one disk through CHARLIE. One disk of mystery and intrigue. Thank you.

Not much a business letter this time. Just formalities. We consider Site-9 cancelled. And we are sure You remember: our next contact is due at ELLIS. Frankly, we are looking forward to JUNE. Every new season brings new expectations. Enclosed in our today's package please find \$10,000. Thank You for Your friendship and help. We attach some information requests. We hope You'll be able to assist us on them. Take care and good luck.

Sincerely,

Your friends.

The KGB asked for information about several specific classified matters, including US Intelligence Community plans to respond to domestic turmoil in the Soviet Union and new United States communications intelligence efforts.

"ELLIS"

In November 1985, Hanssen sold his home on Whitecedar Court when he moved to New York to undertake his new assignment in the FBI field office there. He returned to FBI Headquarters in August 1987, and moved into a home at 9414 Talisman Drive, Vienna, Virginia, which he had bought in July 1987.

In August 1989, the KGB designated drop site "ELLIS," located near Foxstone Park in Vienna, Virginia. The frequent use of this site—at least seven times—illustrates that it might have been chosen for its convenience. Hanssen told the KGB in October 1989 that the KGB could use the "ELLIS" site at any time. In fact, the "ELLIS" site is an approximately one-mile walk from HANSEN's Talisman Drive residence.

Hanssen and the KGB first used the “ELLIS” dead drop on Monday, 23 October 1989. The package to the KGB contained an exact duplicate of the sixteenth diskette (“D-16”), which Hanssen had sent by mail the week before. The diskette contained additional classified information about the US capability to read certain Soviet communications and recruitment matters. Hanssen requested the KGB to load the “ELLIS” site at any time, and advised that he would check the signal site periodically about the loading.

The KGB package contained \$55,000 cash and a letter advising Hanssen that \$50,000 had been deposited into his escrow account in Moscow. Hanssen never signaled that he had cleared this dead drop, and on October 26 the KGB retrieved its package.

The KGB reloaded “ELLIS” on Tuesday, 31 October 1989. Besides the package containing the \$55,000 in cash, the KGB also passed its second diskette. The diskette provided a new accommodation address and instructions to Hanssen on how to inform the KGB of which materials should be opened by the KGB in Washington, D.C., and which should go to the Center. It again conveyed regards from the KGB Chairman and made extensive requests for additional information concerning particular United States intelligence activities targeting the Soviet Union.

On 11 November 1989, the KGB observed that the “ELLIS” signal site was removed, indicating that Hanssen had removed the KGB’s package.

On Monday, 21 May 1990, the KGB loaded the “ELLIS” deaddrop site with a package containing two KGB diskettes, and marked a call-out signal for Hanssen. Hanssen picked up the KGB’s package, but did not leave one for the KGB. The KGB diskettes contained a letter that discussed in detail communications plans and recontact procedures. It read, in part:

Dear Friend:

Congratulations on Your promotion. We wish You all the very best in Your life and career. We appreciate Your sympathy for some difficulties our people face - Your friendship and understanding are very important to us. Of course You are right, no system is perfect and we do understand this. Speaking about the systems. We don’t see any problem for the system of our future communications in regard to this new circumstances of Yours. Though we can’t but regret that our contacts may be not so regular as before, like You said. We believe our current commo plan - though neither perfect - covers rather [sic] flexibly Your needs: You may have a contact with us anytime You want after staying away as long as You have to. So, do Your new job, make Your trips, take Your time. The commo plan we have will still be working. We’ll keep covering the active call out signal site no matter how long it’s needed. And we’ll be in a ready-to-go mode to come over to the drop next in turn whenever You are ready: that is when You are back home and decide to communicate. All You’ll have to do is to put Your call out signal, just as now. And You have two addresses to use to recontact us only if the signal sites for some reason don’t work or can’t be used. . . . But in any case be sure: You may have a contact anytime because the active call out site is always covered according to the schedule no matter how long you’ve been away. . . . Thank You and good luck.

Sincerely,

Your friends.

The KGB particularly asked Hanssen to “give us some good leads to possible recruitments” among “interesting people in the right places.” The KGB also asked for information about a Soviet Embassy employee who Hanssen had previously identified as an FBI recruitment-in-place, and whom the KGB believed was about to defect.

On Monday, 15 July 1991, after a call-out signal from Hanssen, he and the KGB completed an exchange operation at “ELLIS.” The package from Hanssen contained his twenty-third diskette (“D-23”) and approximately 284 pages of material.

The diskette read, in part, “I returned, grabbed the first thing I could lay my hands on” and “I was in a hurry so that you would not worry, because June has passed, they held me there longer.” He also noted that he had at least five years until retirement—he was eligible for retirement in

1996—and remarked “Maybe I will hang in there for that long.” Hanssen also reported on a particular FBI-CIA operation. The classified documents passed included FBI documents, human intelligence plans, and documents concerning nuclear and missile weapons proliferation.

Hanssen returned on 24 May 1991 from a lengthy overseas inspection tour.

The package from the KGB contained \$12,000 cash and a KGB diskette reading, in part, as follows:

Dear friend:

Acknowledging the disk and materials . . . received through “DORIS” we also acknowledge again Your superb sense of humor and Your sharp-as-a-razor mind. We highly appreciate both. Don’t worry. We will not steam out incorrect conclusions from Your materials. Actually, Your information gratefully [sic] assisted us in seeing more clearly many issues and we are not ashamed to correct our notions if we have some. So, thank You for Your help. But if some of our requests seem a bit strange to You, please try to believe us there were sufficient reasons to put them and that what we wanted was to sort them out with Your help.

In regard to our “memo” on Your security. Just one more remark. If our natural wish to capitalize on Your information confronts in any way Your security interests we definitely cut down our thirst for profit and choose Your security. The same goes with any other aspect of Your case. That’s why we say Your security goes first. . . . We are sure You remember our next contact is due at “FLO”. As always we attach some information requests, which are of current interest to us. We thank You and wish You the very best.

Sincerely,

Your friends.

Enclosed in the package please find \$12,000.

The KGB provided new communications plans and made numerous specific requests for classified technical, operational, and recruitment matters. The KGB also asked follow-up questions about information Hanssen had previously provided, and requested specific United States Intelligence Community activity toward the Soviet Union.

“FLO”

As requested by Hanssen the KGB loaded “FLO” on Monday, 3 September 1990, with a package containing \$40,000 cash, and a KGB diskette containing a letter, which identified more call-out signal sites and contained numerous specific requests for classified information. The letter noted that some of the materials Hanssen had provided about “political issues of interest . . . were reported to the very top.” Hanssen subsequently picked up the KGB’s package.

On Monday, 19 August 1991, after a call-out signal from Hanssen, he and the KGB carried out an exchange operation at “FLO.” The package to the KGB contained a recent FBI memorandum concerning a proposed technical surveillance operation of a particular Soviet intelligence officer.

On 1 July 1991, Hanssen returned to the Intelligence Division at FBI Headquarters (after his tour of duty on the Inspection Staff) and became the Headquarters supervisor responsible for FBI coverage of this suspected Soviet intelligence officer.

The package also included the fact that the FBI was initiating a “dangle” operation against the Soviets at a particular named US military facility. Another document provided information that NSA was reading communications of a specific foreign country and the specific methods used to do so.

In addition, the package contained Hanssen’s twenty-fourth diskette (“D-24”) on which he discussed communications plans and provided information about classified technical and operational matters. On this diskette, he also discussed how the Soviet Union could benefit from a thorough study of the period of Chicago’s history when Mayor Richard J. Daley governed the city.

The package from the KGB contained \$20,000 cash and a message welcoming Hanssen back from his overseas inspection trip saying, “it’s great for you to touch the green, green grass of home.” They advised that the next exchange would be at the “GRACE” dead drop site.

“GRACE”

On Monday, 7 October 1991, after a call-out signal from Hanssen, he and the KGB carried out an exchange operation at “GRACE.” The package to the KGB contained his twenty-fifth diskette (“D-25”) and a classified document entitled “The US Double-Agent Program Management Review and Policy Recommendations” dated 10 September 1991. On the diskette, Hanssen provided information about various classified recruitment operations. He also identified by name a particular “old friend” whom he suggested the KGB try to recruit; he explained that the man was a military officer who had recently been told he would not be promoted. (Hanssen has been friends with this individual since he was a teenager.)

The package from the KGB contained \$12,000 cash and a KGB diskette reading, in part, as follows:

Dear friend:

Thanks for the package of 02.13. [The] materials are very promising, we intend to work on the scenario so wisely suggested by You. And the magical history tour to Chicago was mysteriously well timed. Have You ever thought of foretelling the things? After Your retirement for instance in some sort of Your own “Cristall [sic] Ball and Intelligence Agency” (CBIA)? There are always so many people in this world eager to get a glimpse of the future.

But now back to where we belong. There have been many important developments in our country lately. So many that we’d like to reassure You once again. Like we said: we’ve done all in order that none of those events ever affects Your security and our ability to maintain the operation with You. And of course there can be no doubt of our commitment to Your friendship and cooperation which are too important to us to loose [sic]. . . . Please note: our next contact is due at HELEN.

Enclosed in the package please find \$12,000 and attached as always are some information requests which we’d ask Your kind attention to. Thank You and good luck.

Sincerely,

Your friends.

The KGB provided new communications plans and asked for specific information about a variety of classified technical, operational, and analytical matters. The KGB also asked for the current 1991 issue of a particular document reporting on Soviet knowledge of United States satellite reconnaissance systems, commenting that “It’s fun to read about the life in the Universe to understand better what’s going on on our own planet.” Asking about some pages that appeared to be missing from Hanssen’s July package, the KGB noted, “Sometimes it happens, we understand. Life is becoming too fast.”

“LEWIS”

On 12 February 2001, FBI surveillance personnel checking the “LEWIS” deaddrop site found a package concealed at the site. FBI personnel removed the package and transported it to the FBI Laboratory, where it was opened, its contents were examined and photocopied, and it was restored to an apparently intact condition. The package was then replaced at the deaddrop site. The package contained \$50,000 in used \$100 bills and a typed note reading “Next 10/31/01 TOM alt. 20,27.” These were wrapped in white paper, which was taped, and which in turn was wrapped in a taped-up black plastic trash bag inside a second black plastic trash bag.

Escrow Account in Moscow

On 29 September 1987, the KGB deposited \$100,000 into an escrow account established for Hanssen in a Soviet bank in Moscow.

On 22 August 1988, the KGB deposited \$50,000 in an escrow account at a Moscow bank.

The KGB deposited another \$50,000 into Hanssen’s escrow account in a Moscow bank on 17 August 1989.

The End Game

FBI surveillance personnel observed Hanssen driving four times past the Foxstone Park sign on Creek Crossing Road in Vienna, Virginia, on Tuesday evening, 12 December 2000. The Foxstone Park sign is the signal site associated with the “ELLIS” deaddrop site.

That same evening FBI surveillance personnel observed Hanssen walking into a particular store at a shopping center near Foxstone Park at the same time as a known SVR officer was in front of the store.

Two weeks later, on Tuesday, 26 December 2000, FBI surveillance personnel observed Hanssen three times at the Foxstone Park signal site:

1. At approximately 5:42 p.m., Hanssen stopped his vehicle in front of the Foxstone Park sign for approximately 10 to 15 seconds.
2. At approximately 8:53 p.m., Hanssen parked his car on a street off Creek Crossing Road and walked to the Foxstone Park signal site. Hanssen stopped in front of the Foxstone Park sign, holding a lit flashlight, and swept the flashlight beam in a vertical motion over some wooden pylons located near the sign, between the road and the sign. He appeared to the FBI surveillance personnel to focus his flashlight beam on one of the pylons. He then turned and walked away, shrugging his shoulders and raising his arms in a gesture of apparent disgust or exasperation. Hanssen returned to his vehicle and drove away to a nearby Tower Records store.
3. At approximately 9:32 p.m., Hanssen drove back to the Foxstone Park signal site, stopped his vehicle in front of it for approximately two to three seconds, and then drove away.

During January 2001, FBI surveillance personnel observed Hanssen driving pass the Foxstone Park signal site—either slowing or stopping at the site—on three occasions.

1. At approximately 8:18 p.m. on Tuesday, 9 January 2001, Hanssen drove to the Foxstone Park signal site, came to a complete stop in front of it for approximately 10 seconds, then drove away.
2. Shortly before 6:00 p.m. on Tuesday, 23 January 2001, Hanssen drove pass the Foxstone Park signal site, came to a rolling stop near it and then drove away.
3. After 5:00 pm on Friday, 26 January 2001, Hanssen drove pass the Foxstone Park signal site, slowing down near it.

On 30 January 2001, pursuant to court authorization, the FBI searched Hanssen’s Ford Taurus automobile, and found the following:

1. In the glove compartment were a roll of white Johnson & Johnson medical adhesive tape and a box of Crayola colored chalk containing 12 pieces of chalk.
2. In one of four cardboard boxes in the trunk were seven classified documents printed from the FBI’s Automated Case Support (ACS) system. Several pertained to ongoing FBI foreign counterintelligence investigations and were classified SECRET.
3. In another cardboard box in the trunk were six green fabric-covered US Government notebooks containing classified information.
4. Also in the trunk were a roll of Superior Performance Scotch clear mailing tape, and dark-colored Hefty garbage bags.

These items were not removed, although small samples were taken, and they were photographed.

On the evening of Monday, 5 February 2001, FBI surveillance personnel observed Hanssen driving pass the Foxstone Park signal site three times between approximately 5:37 p.m. and approximately 7:44 p.m. That same day, pursuant to court authorization, the FBI searched Hanssen's current personal office within Room 9930 at FBI Headquarters. Hanssen's briefcase, located in the office, contained (1) his current valid US tourist passport; (2) a personal address book; (3) several personal checkbooks; (4) multiple sets of financial statements; (5) one computer floppy disk; (6) one 8MB Versa Card Flash Memory Adapter, which is a memory storage card for a computer; and (7) one cell phone. These items were photographed, duplicated, or otherwise recorded, but not removed or altered. Upon examination, the FBI determined that the memory storage card contained several letters associated with the "B" operation. Because these letters were found in Hanssen's possession proved that Hanssen was "B."

On 12 February 2001, pursuant to court authorization, the FBI again searched Hanssen's Ford Taurus automobile. In addition to the items described in part (1) of the foregoing paragraph, the glove compartment contained a small plastic box containing thumbtacks of various colors, including yellow and white. It was further ascertained that at least one of the pieces of chalk was pink. These items were not removed, although small samples were taken, and they were photographed. During this search, Hanssen's briefcase was observed in the vehicle, but it was not removed.

At approximately 4:21 p.m. on 18 February 2001, FBI surveillance personnel observed Hanssen drive his car into the parking lot of the Pike 7 Plaza shopping center at Route 7 and Gosnell Road at Tysons Corner, Virginia. He stopped his car, got out, walked to the trunk and opened it. He removed a black plastic trash bag into which he placed something. He got back into his car and, after a brief period, drove away.

Thirteen minutes later, Hanssen arrived at the ELLIS signal site. He got out of his car and placed a piece of white adhesive tape on the Foxstone

Park sign, then began to walk into the wooded park in the direction of a footbridge. Approximately nine minutes later, Hanssen walked back out of the wooden area, where the FBI arrested him. When arrested, Hanssen was carrying his FBI credentials and a small roll of white adhesive tape.

FBI agents recovered from under the footbridge a package wrapped in a taped black plastic trash bag. The package was taken to the FBI laboratory where it was photographed, opened, and its contents examined.

Inside the package was a computer diskette containing an encrypted letter, which, when decrypted, read as follows:

Dear Friends:

I thank you for your assistance these many years. It seems, however, that my greatest utility to you has come to an end, and it is time to seclude myself from active service.

Since communicating last, and one wonders if because of it, I have been promoted to a higher do-nothing Senior Executive job outside of regular access to information within the counterintelligence program. It is as if I am being isolated. Furthermore, I believe I have detected repeated bursting radio signal emanations from my vehicle. I have not found their source, but as you wisely do, I will leave this alone, for knowledge of their existence is sufficient. Amusing the games children play. In this, however, I strongly suspect you should have concerns for the integrity of your compartment concerning knowledge of my efforts on your behalf. Something has aroused the sleeping tiger. Perhaps you know better than I.

Life is full of ups and downs.

My hope is that, if you respond to this constant-conditions-of-connection message, you will have provided some sufficient means of re-contact besides it. If not, I will be in contact next year, same time same place. Perhaps the correlation of forces and circumstances then will have improved.

Your friend,

Ramon Garcia.

Also inside the package were seven FBI documents printed from the FBI's ACS system, classified SECRET and dated from October through December 2000, relating to recent activity in ongoing FBI foreign counterintelligence investigations against Russia targets.

On 10 May 2002, Robert P. Hanssen was sentenced to life in prison without parole for two decades of spying for Moscow. The 58-year-old former FBI counterintelligence agent read a short, carefully worded statement in an Alexandria, Virginia, Federal courtroom apologizing for his betrayals of his family and country. Hanssen, a 25-year veteran of the FBI, evaded detection for decades and caused incalculable damage to US intelligence efforts. A plea agreement in July 2001 spared Hanssen the death penalty in exchange for his cooperation. The CIA and Justice Department have “serious reservations” about Hanssen’s cooperation during repeated interrogations, but FBI investigators are satisfied with his level of cooperation. Under the plea agreement, Hanssen’s wife will receive the survivor’s portion of his FBI pension and retain the family home in Vienna, Virginia.

Endnotes

¹ The Komitet Gosudarstvennoy Bezopasnosty, known as the KGB, was the intelligence service of the Soviet Union. In December 1991, the Sluzhba Vneshney Razvedki Rossia, known as the SVR, assumed the foreign intelligence functions of the former KGB for the Russian Federation. Both terms are used in this document to refer to activities of either the KGB or the SVR.

² The ACS is the FBI’s collected computerized databases of investigative files and indices. ACS came online in October 1995. The main and most extensive ACS database is the Electronic Case File (ECF), which contains electronic communications and certain other documents related to ongoing FBI investigations, programs, and issues and the indices to those documents. It is the equivalent of a closed FBI Intranet. ACS users can access individual files by making full-text search requests for particular words or terms. FBI personnel who are “approved users” of ACS, including Hanssen, must log on with a user identification number and password unique to each user. Retrieval logs make it possible to conduct audits of individuals’ use of ACS.

³ The FBI recorded a portion of the 18 August 1986 telephone call between KGB Officer Aleksander Fefelov and “B.” Two FBI analysts, who worked closely and routinely with Hanssen for at least five years, listened to both the recording and an FBI-enhanced version of the recording in which background noise was minimized. They have both concluded without reservation that the voice of “B” is that of Hanssen.

⁴ When “B” made deaddrops to the KGB/SVR, he would place the contents of the drop in a plastic garbage bag, which he would wrap with tape. The plastic bag would then be placed inside a second garbage bag. The FBI came into possession of the inner plastic bag used by “B” on one occasion to wrap the contents of a package to the KGB. A FBI fingerprint examiner conducted an examination of the plastic bag and ascertained that it contains two latent fingerprints of comparison value. The examiner determined that these two fingerprints are those of Hanssen.

Russian Counterintelligence Begins Comeback

20 December 2001 marked the 84th anniversary of the Cheka—the Soviet secret police.

Introduction

The history of the Soviet Union/Russia is a history of its state security establishment. In no other country has intelligence and security services performed such a crucial or extensive mission in sustaining a government, so manipulated the lives and destiny of its citizens, or been so committed in enforcing the will of the governing on those being governed. The first of many internal security groups was the Cheka, which Vladimir Lenin used to consolidate the Communist hold on the Soviet Union. According to Lenin, no law except the defense of the revolution bound the Cheka.

Since the turbulent days of the Cheka, the Soviet state security organs, with its periodic name changes, remained the Communist Party's primary instrument for maintaining itself in power, and counterintelligence has always been the key element to protect the government. Its task is to identify domestic opponents, neutralize opposition to the government, control the media, and protect state secrets where anything can be defined as a state secret. While counterintelligence monitors foreign representatives and travelers, its overwhelming focus is on national problems.

After the fall of the Soviet Union, the KGB was abolished and its responsibilities distributed to several agencies. The SVR inherited the foreign intelligence role, FAPSI (Federal Agency for Government Communications) inherited the SIGINT intercept role, and the Border Guards maintained its watch over the borders but as a separate agency.

The internal security functions previously performed by the KGB's Second, Third, and Fifth Chief Directorates and the Seventh Directorate were initially assigned to a new Ministry of Security, Ministerstvo Bezopasnosti Ruskii

(MBR). Col. Gen. Viktor Barranikov, a career law-enforcement officer who joined the Ministry of Internal Affairs (MVD-Ministerstvo Vnutrennikh Del) in 1961, directed the MBR. Barranikov reported to the Russian Federation Security Council—established in April 1992. Press reports placed the number of MBR staff members at 137,900 as of mid-1992.

Yeltsin Begins CI Reorganization

In December 1991, Yeltsin issued a decree merging the MBR (then called the Federal Security Agency) with the MVD. The two agencies were to coexist as the Ministry of Security and Internal Affairs. However, after reviewing the merger decree, the Russian Constitutional Court declared it unconstitutional and advised Yeltsin to annul it. He complied.

Although Yeltsin complied with the court's decision, his administration was not happy. Sergei Shakray, legal adviser to Yeltsin, criticized the court for exceeding its mandate by questioning an administrative decision fully within the President's authority to make. Interestingly, a Constitutional Court Justice argued that a merged security agency would be more difficult to supervise than two separate organizations. Although the Yeltsin circle never elaborated their counter-argument—that unification under the right leader would permit faster reform and reduce costs—Yeltsin did, however, appoint Barranikov and Viktor Yerin, the presumed senior managers of the joint agency, as head of the MBR and the MVD, respectively.¹

In February 1992, the parliament undertook a study to recommend the manner in which effective political control over the MBR could be ensured.

The Ministry of Security was responsible for analyzing threatening foreign situations, conducting counterintelligence and collecting intelligence in cooperation with the SVR, monitoring and protecting joint economic ventures, and defending the military forces and foreign establishments in Russia, as well as space,

engineering, army, and strategic assets. However, despite its broad mandate, the MBR was said to not monitor the political activity of Russian citizens.

But in the fall of 1992, the MBR detained Vil Mirzayanov on the charge of disclosing state secrets. Mirzayanov had publicly written that Russia was working on a nerve gas weapon, which questioned Yeltsin's statement in January 1992 that Russia would comply with the US-Soviet agreement on nonproliferation of chemical weapons. Vladimir Uglev, who was one of the chief chemical weapons designers, corroborated Mirzayanov's allegations though no charges were filed against Uglev for revealing state secrets because he had deputy's immunity as an elected official.

After President Yeltsin became uncertain of the Ministry's loyalties during his struggle with parliament, the MBR was disbanded in December 1993 and replaced by the Federal Counterintelligence Service [Federal'naya Sluzhba Kontr-razvedky - FSK].

On 3 April 1995, Yeltsin signed a new law, passed by the Duma, to create the Federal Security Service (FSB—Federalnaya Sluzhba Bezopasnosti) to replace the FSK. Under the new law, the FSB had enhanced authority to combat the Russian Mafia, almost unlimited authority to conduct operational searches and the approval to conduct foreign intelligence operations.

In mid-1995, Yeltsin decided he needed to take action against the FSB. The security agency's failures in Chechnya and the mid-June Budennovsk hostage drama were the most obvious grounds for Yeltsin's shakeup. The shakeup was also motivated by Yeltsin's perception that the FSB was insufficiently loyal to him politically. The day after the 29 June 1995 Security Council meeting at which Yeltsin criticized the FSB for failure to prevent the Budennovsk attack, Yeltsin accepted Sergey Stepashin's resignation as FSB director.²

Barsukov Takes FSB's Reins

On 24 July 1995, Yeltsin chose his own close protege Mikhail Barsukov to head the FSB.³ When Yeltsin presented the new director to FSB leaders on 24 July,⁴ he delivered a 50-minute speech calling on the FSB to work more effectively⁵ and harshly criticizing Stepashin and FSB Deputy Director Igor Mezhaikov, who supervised Chechen operations as deputy director for crisis situations.⁶

Yeltsin apparently also had other, more political grounds for dissatisfaction with the FSB under Stepashin, however, as his close proteges Aleksandr Korzhakov and Barsukov were clearly critical of Stepashin and his agency. FSB personnel, in turn, apparently resented the power of Korzhakov's Security Service of the President (SBP) and Barsukov's Main Protection Directorate (GUO), which had taken over some former KGB functions well beyond those of protection agencies (for example, control of the Alfa antiterrorism unit).

Even before the Chechen war, relations between Stepashin and his FSB and Korzhakov were bad, and Yeltsin reportedly threatened to merge the FSB with the SBP and GUO.⁷

The December 1994 raid on the Most Bank by Korzhakov's SBP and Barsukov's GUO led to a shootout with the Moscow FSB and to Yeltsin's firing—at the urging of Korzhakov and Barsukov—Stepashin's deputy, Yevgeniy Savostyanov, as Moscow FSB chief. Stepashin reportedly threatened to resign in protest.⁸

The failures in Chechnya increased Yeltsin's dissatisfaction with FSB work and spurred further rumors of a shakeup.⁹ Stories were later spread that Stepashin was hesitant even to order an all-out hunt for Chechen rebel leader Dzhokhar Dudayev, fearing heavy loss of life in such an effort.¹⁰

Resentment against Barsukov and Korzhakov was openly expressed by intelligence specialists formerly associated with the security agencies in a White Book of Russian Special Services (Belaya Kniga Rossiyskikh Spetssluzhb) printed

in July 1995. The book's authors complained that Korzhakov's SBP and Barsukov's GUO had taken over some of the old KGB functions that, they felt, legitimately belonged to the FSB. They criticized Korzhakov's SBP for becoming a "powerful mini-KGB," with Korzhakov seeking the role of "doyen" of the whole security community. They also complained that the SBP had been given the right to conduct investigations and the right to oversee arms sales, foreign currency exchange, and other "profitable spheres" of economic activity.

The book's authors criticized the subordination of the FSB directly to the president (pages 31, 44-45). Among the many authors listed as contributing to the book were Stepashin and former KGB leaders Vladimir Kryuchkov and Fedor Bobkov. Aleksey Podberezkin—a leading Communist Party official and no friend of the Yeltsin regime, who may have unduly emphasized the complaints against Yeltsin and his aides, headed the collective of authors that actually drafted the book.

Yeltsin's appointment of Barsukov led to a number of other high-level personnel changes in the FSB. He accompanied his appointments with a 24 July 1995 edict decreeing that the FSB would now have two first deputy directors—it had only one previously—and six deputy directors.¹¹

At the same time he appointed Barsukov, Yeltsin appointed a new first deputy, Col. Gen. Viktor Zorin, chief of the Directorate for Counterintelligence Operations.¹² As head of the FSB's biggest unit,¹³ Zorin was well acquainted with FSB operations and could aid the outsider Barsukov as he took over.¹⁴ Zorin reportedly had the support of Korzhakov,¹⁵ having gained Korzhakov's favor by suggesting a coordination agreement between the SBP and FSK in May 1994 that appeared to enhance the SBP's status.¹⁶

In addition to Zorin, Yeltsin promoted Anatoliy Trofimov, head of the Moscow FSB, from deputy director to first deputy director. Trofimov, who was viewed as willing to follow Korzhakov's lead, was only six months before named Moscow security

chief and FSK deputy director to replace Yevgeniy Savostyanov, who had been fired. The then present deputy director Anatoliy Safonov, who had been acting director since Stephashin's removal, was left without a job.¹⁷

Yeltsin's appointment of Barsukov engendered little public criticism despite its apparent boost to Korzhakov, whose empire-building and reputed influence with Yeltsin had been repeatedly attacked in the Moscow press. Presidential Administration Leader Sergey Filatov, who had demonstrated concern over Korzhakov's growing power, praised Barsukov's management of the GUO, predicted he would run the FSB well also, and denied that Barsukov's appointment would mean that the FSB would be used to help the president's reelection.¹⁸ Duma Security Committee Chairman Viktor Ilyukhin, usually a hardline critic of Yeltsin, called the appointment "natural" and did not publicly criticize it.¹⁹

A second round of changes occurred in September, when Yeltsin and Barsukov fired Deputy Director Mezhaikov, Chief of the Directorate for Fighting Terrorism; Gen. Anatoliy Semenov; and Stavropol FSB Chief Romanov,²⁰ apparently as scapegoats for Chechnya and Budennovsk. Barsukov confirmed that they had been removed "by a presidential decree after the events in Budennovsk."²¹ Mezhaikov's removal was particularly noteworthy because he is the brother-in-law of the powerful First Deputy Premier Igor Soskovets²² and had headed the FSK Cadres Directorate before being promoted to deputy director and put in charge of Chechnya.²³ He also fired Colonel Semenov, FSB Chief of the Directorate for Combating Terrorism.

Also in September, Barsukov fired Maj. Gen. Anatoliy Krayushkin, chief of the Directorate for Registration and Archives, for failures in his work.²⁴ Several of Krayushkin's subordinates had been arrested for illegally issuing visas.²⁵ Krayushkin, like the dismissed Semenov and Mezhaikov, was a member of the collegium of the FSB and thus became the third member of this 12-man body to be removed under Barsukov.²⁶

In addition to personnel changes, Barsukov began making changes in FSB structure, with Yeltsin's mandate to strengthen the FSB and expand its powers and activities. The confirmed changes were all related only to Chechnya and the threat of terrorism.

To build up an antiterrorism force in the FSB, the Alfa antiterrorist unit formerly in the KGB was transferred from the GUO to the FSB. While the early August Yeltsin edict ordering this transfer was not published, Barsukov reportedly read the order to Alfa personnel,²⁷ and the transfer was confirmed by a GUO spokesman on 11 August.²⁸ Sergey Goncharov, president of the Alfa Veterans Association, credited Barsukov with returning Alfa from the GUO.²⁹

Shortly afterward, it was decided to create a new Anti-Terrorism Center out of the Directorate for Combating Terrorism and the Alfa unit.³⁰ A 14 September Yeltsin edict named First Deputy-Director Zorin chief of the Anti-Terrorism Center.³¹ Barsukov reported to Yeltsin on progress in creating the Anti-Terrorism Center on 18 September and 6 December.³²

Other proposals for expanding FSB activities that would clearly impinge on other security agencies were suggested but were not approved or put into effect:

- On 28 September 1995, Komsomolskaya Pravda reported that a draft Yeltsin edict had been prepared, giving the FSB additional rights to check the work of the Internal Affairs Ministry (MVD), the Federal Agency for Government Communications and Information (FAPSI), tax police, and other security organs and watch for corruption in their ranks. On 22 November, NTV reported that the "State Security Service" (presumably the FSB) was setting up a unit in the MVD to monitor its staff and clean up corruption.
- On 3 November, Moskovskiy Komsomolets reported that Barsukov planned to create other centers in addition to the Anti-Terrorism Center—a Center for Counterespionage, a Center for Combating Organized Crime, and an

Operational Center. The Center for Combating Organized Crime would appear to overlap with the MVD's Main Directorate on Organized Crime, but a new head for this directorate was recently appointed, suggesting that plans to transfer it out of the MVD or downgrade it are not imminent. Valeriy Petrov was named first deputy internal affairs minister and head of the Main Directorate on Organized Crime in November.³³

- On 11 November, Moskovskiy Komsomolets cited unnamed "sources," claiming that Barsukov had decided to create a new directorate dealing with foreign intelligence.³⁴ FSB involvement in foreign intelligence became the subject of hot debate in the Duma in December as it considered a law on foreign intelligence. The law for the first time defined the spheres of the SVR, the armed forces' Main Intelligence Directorate (GRU), FAPSI, and the Federal Border Service in foreign intelligence, but "after long debate" a provision permitting the FSB to have its own foreign intelligence service was excluded from the law.³⁵

Some press reports have even claimed that Yeltsin gave Barsukov license to virtually recreate the KGB by subsuming other security agencies under the FSB:

- Moskovskiy Novosti (30 July-6 August 1995) reported that "sources close to the FSB" said an edict was being prepared to put the GUO and FAPSI into the FSB and that such a reorganization had been Barsukov's condition for accepting the post of FSB director.
- Argumenty i Fakty (No. 31, August 1995) quoted "competent sources" saying that Barsukov came "with a blueprint for the resurrection of the KGB, approved by the president." This plan reportedly would bring the SVR and Federal Border Service into the FSB.
- Obshchaya Gazeta (17-23 August 1995) cited sources in the MVD claiming that a plan to put the MVD's Main Directorate on Organized

Crime and the Federal Border Service into the FSB was under consideration. Mikhail Yegorov resigned as first deputy internal affairs minister and head of the MVD Main Directorate on Organized Crime on 18 August 1995,³⁶ and no one was named head of the directorate until November, perhaps encouraging the idea it would be abolished or transferred to the FSB.

- Komsomolskaya Pravda (22 August 1995) said that units of FAPSI and the SVR would soon be transferred to the FSB.

None of these major reorganizations occurred, and the chiefs of the SVR (Yevgeniy Primakov), FAPSI (Aleksandr Starovoytov), the Federal Border Service (Andrey Nikolayev), and MVD (Anatoliy Kulikov)—all of whom were directly subordinate to Yeltsin—would surely have resisted having their agencies dissolved into the FSB.

The changes within the FSB became increasingly hard to track in the media because Barsukov imposed stricter secrecy over the agency's inner workings. Stepashin had been relatively open, granting interviews and apparently allowing FSB officials to talk to reporters.³⁷ After Barsukov took over, officials of the FSB's Public Relations Center announced that all data on FSB personnel and leadership changes were now considered military secrets,³⁸ and Barsukov ordered his subordinates to cease contact with the press.³⁹ On 7 December, Komsomolskaya Pravda reported that Barsukov had issued a secret order forbidding all special services personnel—except for the FSB Public Relations Center—from having any contact with the media.

Protection of State Secrets Upgraded

Coincident with Barsukov's takeover and the strengthening of the FSB, another step was taken to tighten control over state secrets—the 9 November 1995 creation of an Interdepartmental Commission for Protecting State Secrets. The reorganization was announced in an edict that Yeltsin signed while still in the hospital. He named First Deputy Premier Oleg Soskovets as chairman and Barsukov

and State Technical Commission Chairman Yuriy Yashin as deputy Chairmen.⁴⁰ The creation of an interdepartmental commission headed by a first deputy premier represented a significant upgrading of the bureaucracy charged with protecting state secrets, until then led by the lower-level State Technical Commission, headed by Yashin.⁴¹

The change benefited Barsukov since it established his agency's priority role in protecting secrets. As deputy chairman of the commission, he now clearly outranked heads of all other agencies in the field of protecting state secrets—the Defense Ministry, FAPSI, the SVR, and so forth—except for fellow Deputy Chairman Yashin.

In another boost to Barsukov, Yeltsin signed an edict the same day, promoting him to General of the Army.⁴² The promotion may have been partly prompted by a desire to give Barsukov equal rank to General Yashin. In any case, the promotion was another sign of Yeltsin's favoritism toward Barsukov, since his predecessor as FSB director, Stepashin, was only a lieutenant general when removed in July. The edict promoting Barsukov was signed on 9 November as Barsukov visited Yeltsin in the hospital, perhaps as a gift for Barsukov's 8 November birthday.⁴³

In addition to boosting Barsukov personally, the creation of the new commission appeared to further the campaign the FSB had been pushing to enhance vigilance and suspicion toward foreigners. The campaign surfaced in January with press publication of warnings from the FSK—predecessor to the FSB—about foreign spying and subversion.⁴⁴ Stories that were leaked to the press continued to promote the need to protect state secrets. For example, on 23 September, Komsomolskaya Pravda published an article criticizing the Duma's foreign affairs committee for selling nonsecret but possibly sensitive Duma draft documents to Westerners.

As the campaign continued, the FSB became more aggressive in harassing those suspected of gathering Russian information. For example, in October the FSB charged the nongovernment

Norwegian Bellona environmental organization with possessing files containing secret data on the Russian Navy and merchant marine.⁴⁵ Other FSB actions and items in the press also appear part of this vigilance campaign.

Barsukov appeared to have particularly strict views on keeping information secret. An 11 October Moskovskiy Komsomolets article reported that he was more hostile to the press even than Security Service of the President Chief Korzhakov, refusing to give any interviews at all and insisting that all information about FSB personnel is classified. The article said that his secretive mentality was reflected in his assumption of full personal control over issuing of passes to “all employees of structures having anything to do with state secrets.”

Although pressure from Barsukov and his campaign for heightened vigilance probably account for the timing of the 9 November edict, the creation of the interdepartmental commission had been planned for a long time but not carried out. The law “On State Secrets” enacted in July 1993 had provided for working out a program for protecting secrets and for an Interdepartmental Commission for Protecting State Secrets.⁴⁶ The body was not created, and on 30 March 1994, Yeltsin signed an edict authorizing the State Technical Commission to temporarily carry out the duties assigned to the interdepartmental commission.⁴⁷ The continued failure to set up the interdepartmental commission was attested to by later laws—the 20 February 1995 statute on the system for declassifying archive documents⁴⁸ and the 4 September 1995 rules⁴⁹ for classifying state secrets—that assign tasks to the interdepartmental commission but note that the State Technical Commission is acting temporarily for the commission. Yashin, in a 12 August 1995 Krasnaya Zvezda interview, suggested that his agency could continue to supervise protection of state secrets and that no other body needs to be created.

One probable reason for the lack of action on creating an oversight body and on working out rules and procedures for state secrets was competition among the many agencies handling

state secrets. The law “On State Secrets” listed the Defense Ministry, Ministry of Security, FAPSI, SVR, and State Technical Commission as agencies that protect state secrets.⁵⁰ It listed the State Committee for the Defense Industry, the Atomic Energy Ministry, Ministry of Science and Technology Policy, Economy Ministry, Justice Ministry, Foreign Affairs Ministry, Communications Ministry, Academy of Sciences, and Russian State Archive as other agencies that classify information and make decisions on secrets.

FAPSI was charged with protecting state secrets in the “Law on Federal Organs of Government Communications and Information.”⁵¹ The FSB was charged by its 23 June 1995 statute with protecting state secrets; licensing enterprises using state secrets; checking the protection of state secrets in state organs, military units, and public and private enterprises; and setting rules for access to state secrets.⁵²

In addition, the Security Council’s Interdepartmental Commission for Information Security was also involved, for example, meeting in March 1994 to discuss implementation of the law “On State Secrets” and on how to create a mechanism for protecting state secrets.⁵³ Yashin and chief of the Russian State Archive Rudolf Pikhoya said 40 agencies were involved in decisions on state secrets.⁵⁴

With so many organizations, officials complained that it was difficult to reach agreement on the rules of secrecy. Yashin complained that his State Technical Commission in December 1994 had prepared a “list of information categorized as state secrets” and sent it for coordination to the 40 agencies responsible for protecting information but that six months later nothing had been accomplished.⁵⁵ Pikhoya complained that declassification of archive documents was hampered because 40 agencies are involved.⁵⁶ One newspaper complained that, ever since the collapse of the old system, controls on secret information have “been in a kind of limbo,” with organizations themselves left to decide what should be kept secret.⁵⁷

In 1995, however, work on tightening control of state secrets moved more rapidly, along with the considerable strengthening of the FSB. The Duma on 25 January passed a law “On Information, Provision of Information, and Protection of Information,” including an extensive section on protection of state secrets and “confidential” documents.⁵⁸

Premier Viktor Chernomyrdin approved a 20 February statute “On Procedure for Declassification of and Prolonging Classification Periods for USSR Government Archival Documents” that ordered creation of an Interagency Group of Experts made up of representatives from 13 agencies and headed by the deputy chairman of the interdepartmental commission. The group was to operate under the interdepartmental commission, but the statute noted that the State Technical Commission was still acting for the interdepartmental commission.⁵⁹ In May, Chernomyrdin signed a decree creating a system of licensing for enterprises dealing with state secrets and ordering the FSB, State Technical Commission, FAPSI, and the SVR to work out the licensing.⁶⁰

On 3 April, Yeltsin signed a law “On Organs of the Federal Security Service in the Russian Federation,” renaming the FSK the FSB and expanding its powers and responsibilities, which included protecting state secrets.⁶¹ Yeltsin approved the 23 June statute on the FSB, defining its powers and tasks, including its detailed tasks in protecting state secrets⁶²

On 26 June, Chernomyrdin approved a statute “On Certification of Means of Protecting Information,” outlining the registration of all cryptographic and other technical means for protecting state secrets.⁶³

The Duma on 5 July passed a new law “On Operational- Investigative Activities,” apparently strengthening the powers of the FSB, the Main Protection Directorate (previously led by Barsukov), Korzhakov’s Security Service of the President, the SVR, the tax police, and other bodies.⁶⁴ Moskovskiy Komsomolets (3 November) asserted that the law had been drawn up within the FSB and its position strengthened.

Chernomyrdin signed a 4 September decree approving “Rules for Defining Information Comprising a State Secret, for Various Levels of Secrecy” worked out on the basis of the law “On State Secrets,” which was published in the 11 September 1995 *Sobraniye* and 14 September 1995 *Rossiyskaya Gazeta*.

With a new interagency commission to coordinate handling of state secrets and with Barsukov’s enhanced role in protecting secrets, the already evident tightening of control over sensitive information would intensify. Although the new rules on secrets likely expanded the types of information considered classified and the State Technical Commission had power all along over political and economic secrets, as well as military and technical secrets, Barsukov appeared to be more aggressive in interpreting the rules on secrets and in enforcing protection of secrets and information he considered should be classified.

Barsukov’s firing of Anatoliy Krayushkin, chief of FSB archives, also reflected a tightening of control over information although press articles have not reported any accusations that Krayushkin wrongly released archive material. However, it was rumored that he had fallen under suspicion in connection with a German intelligence agent.

To strengthen its counterintelligence mission, the FSB turned to the Russian media to send a two-part message: Russian citizens should be careful of contacts with foreigners, and Russians should support the FSB to negate the foreign intelligence threat. This new campaign is reminiscent of previous KGB efforts to alert the public to the nefarious activities of Western spies.

Russia’s mainstream media began to cooperate with the FSB by publishing items touting Russia’s intelligence services and warning that hostile Western intelligence services still pose a threat to Russia’s security. Examples of items reflecting the growing closeness between the security services and the media appeared in both state-owned and independent media, including some media that are usually proreform:

- A 22 September article in *Komsomolskaya Pravda* alleged attempts by a “CIA officer” within the US Embassy in Moscow to poll members of the Moscow academic elite for details on Yeltsin’s personal life.
- A 24 September item from Interfax declared that hostile foreign intelligence activities were on the increase and decried the policies of “openness,” which facilitated the opportunity for contact between Russian citizens and foreign spies.
- A 30 September article in *Komsomolskaya Pravda* lamented the damage to national security, resulting from the sale of Russian satellite photographs to Western firms.
- A 7 October program aired on Russian television featured an interview with a Russian citizen convicted of spying for the West in 1992.
- An 11 October item from ITAR-TASS advertised the publication of a “white book,” hailing the legacy of Russia’s intelligence services.

Such media activity emulated the openly recidivist line that FSB officials used in describing their activities. An article on an “old-timers day” meeting for former KGB officials hosted by newly appointed FSB Director Barsukov asserted—citing Barsukov’s remarks—that Barsukov conceived of his task as “strengthening the role of the service and hardening its policies in a manner worthy of the traditions of the KGB.”⁶⁵ The article also contended that Barsukov was restoring the veil of secrecy surrounding the organization, reporting that the FSB’s Center for Public Relations had recently “shocked” a group of journalists by refusing to comment on recent personnel moves and asserting that “all” information on FSB officers constitutes a “military secret.”

The items also reflected the closer relationship between the media and the security services called for in two acts signed by President Yeltsin. These acts charge the FSB and other security agencies with working jointly with Russian media to accomplish their mission and allow the recruitment of Russian journalists as informants and operatives.

“The Statute on the Federal Security Service of the Russian Federation” approved by Yeltsin on 23 June tasked the FSB in a section titled “FSB Functions” to “organize and conduct interaction with the mass media, inform society on [FSB] activities . . . and conduct editorial-publishing activities.”⁶⁶ The terms of the statute are not defined precisely and appear to be open to broad interpretation.

“The Federal Law on Operational-Investigative Activities” passed by the State Duma on 5 July and signed by Yeltsin on 12 August authorized Russian intelligence organizations to hire journalists as paid informants and agents and lists agencies authorized to do so.⁶⁷ The list included the Ministry of Internal Affairs, the FSB, the SVR, and the federal organs of state protection (defined as the Main Protection Directorate and the Presidential Security Service).

Aleksandr Zdanovich, deputy chief of the FSB’s Center for Public Relations, defended the recruitment of journalists and argued that the media have a civic duty to cooperate with security organs.⁶⁸ Asked about the possibility of journalists becoming “informants” for the FSB and other investigative organizations, Zdanovich called the prospect a “completely normal phenomenon.” He called “rendering assistance to the security organs” by journalists a “constitutional duty” and added that in some cases the failure to report information “in cases of especially dangerous crimes against society” could result in criminal liability for journalists. Zdanovich asserted that “the main thing for us is that we do have paid informants” in journalistic circles, adding that the FSB had “fought” for this law.

Zdanovich also said that the law “On Mass Media,” signed into law by Yeltsin on 27 December 1991, should be modified to make it compatible with the law on investigations. While he did not specify the points of incompatibility in the two laws, he may have been referring to the Law on Investigations’ ban on investigative activities by nonlaw enforcement organizations and individuals, and the Law on the Mass Media’s guarantee of journalists’ rights to “seek, obtain . . . and

distribute” mass information without restriction. In addition, Zdanovich’s implication that journalists could be forced to reveal their sources would clearly contradict the media law’s stipulation that journalists have a “responsibility” to “protect the confidentiality of information and (or) its source.”⁶⁹

The new documents on media activities by the FSB, supported by both Yeltsin and the usually anti-Yeltsin legislature, suggest that Russian media one day would have to yield hard won journalistic freedoms in the alleged interests of Russian national security and social stability. Taken together with the recent appointment of hardliner and long-time Yeltsin loyalist Barsukov, these developments suggest that the traditional domestic espionage and propaganda functions exercised by the Soviet-era KGB were gradually being revived.

Other Security Services Changes

In a 28 July 1995 edict, Yeltsin placed the GUO “under the day-to-day” management of the SBP, giving Korzhakov control of all Kremlin guards and reversing the original relationship of the GUO and SBP. Korzhakov and the SBP had been subordinate to Barsukov until November 1993, when Yeltsin created the SBP as a separate agency out of the GUO.⁷⁰ Korzhakov’s SBP protected the president, while the GUO protected other leaders.

Yeltsin’s edict separated the posts of GUO head and Kremlin commandant—long held concurrently by Barsukov—creating a separate post of deputy GUO head, who would be Kremlin commandant. On 29 July 1995, Yeltsin’s Press Service reported the president named Barsukov’s first deputy, Yuriy Krapivin, to head the GUO and promoted him to lieutenant general.⁷¹ Maj. Gen. Valeriy Nikitin was named first deputy head of the GUO, and Maj. Gen. Sergey Strygin was named deputy head and Kremlin commandant.

At the same time, Yeltsin promoted Korzhakov to lieutenant general, making him equal in rank to the head of the GUO.⁷² Barsukov, as head of the larger GUO, had had a higher rank (colonel general) than Korzhakov, whose SBP was smaller.

Although placing other presidential organs under presidential Administration Leader Filatov in a new edict, Yeltsin reaffirmed Korzhakov’s independent status. In another 28 July edict, “On the Administration of the President of the Russian Federation,” Yeltsin placed the SPB, along with other “state organs led directly by the president,” in Filatov’s Administration of the president but preserved Korzhakov’s independence of Filatov. The edict said that the Administration leader (Filatov) would manage such bodies, but it made an exception for the SBP, saying that the leader of the Administration “does not carry out operational management of the SBP.”⁷³ In the past, the SBP had been outside the Administration and outside Filatov’s control; now it would be within the Administration but still outside Filatov’s control.

While subordinating the GUO to Korzhakov, Yeltsin kept for himself the power to name its two top officers. The 28 July edict specified that the GUO head and deputy head are to be appointed directly by the President.

In addition to the leadership changes in the FSB and GUO, there were also changes in the MVD. A 6 July Yeltsin edict named Col. Gen. Kulikov, deputy internal affairs minister and chief of MVD internal troops,⁷⁴ as the new internal affairs minister.⁷⁵ Lt. Gen. Anatoliy Romanov succeeded Kulikov as deputy minister and commander of internal troops.⁷⁶ Yerin, removed as internal affairs minister on 30 June 1995, was named deputy director of the SVR on 5 July.⁷⁷

FSB Comes Out on Top

Changes to the FSB made it clearly the preeminent security agency, but Yeltsin did not sanction the FSB taking over all former parts of the KGB and recreating a centralized security agency. Yeltsin followed his cautious rule of keeping the security services splintered and directly under his control. Though the FSB, MVD, SVR, GUO, and Border Service had membership in the cabinet, they were directly under the president, and Premier Chernomyrdin had little influence over them.

A revitalized and more politically aggressive FSB under Barsukov, along with Korzhakov's politically active SBP, had the potential to be an important player in the next election for national leadership. However, whatever plan or scenario Yeltsin contemplated for using, the FSB and the SBP unraveled prior to the runoff election.

Yeltsin Fires FSB and SBP Chiefs

Reformers led by former First Deputy Premier Anatoliy Chubays appeared to have maneuvered Yeltsin into firing his three closest hardline deputies—SBP Korzhakov, FSB Director Barsukov, and First Deputy Premier Soskovets—after the hardliners overreached themselves in a clumsy attempt to discredit Yeltsin's reformist deputies and perhaps postpone the runoff elections. The upheaval resulted from the longtime rivalry between the hardline Korzhakov-Barsukov-Soskovets group and reformers such as Chubays, former Yeltsin chief of staff Filatov, and Premier Chernomyrdin. There was also a bitter struggle over leadership of Yeltsin's election campaign between Korzhakov and Soskovets on the one side and Chernomyrdin, Chubays, and First Assistant to the president Ilyushin on the other. The ousters appeared, in the short run at least, to have dramatically boosted the influence of Chernomyrdin, Chubays, and other reformers and also newly appointed security boss Aleksandr Lebed, whose actions have been lauded as saving democracy on his second day in office.

The ouster of Korzhakov and his allies probably only came about because of Chubays's bold gamble. Chubays dragged Lebed into the dispute, tipped off the media, and set off exaggerated reports of a coup and forced Yeltsin to take action by scheduling a news conference to expose the whole dispute. Without such actions, Korzhakov's arrest of Yeltsin's campaign aides probably would have resulted in some charge of corruption against Chubays or else been quietly hushed up.

Korzhakov's fatal maneuver was the 19 June arrests of two Yeltsin campaign aides. The action

appeared to be an attempt to take advantage of an opportunity to incriminate the leaders of Yeltsin's campaign staff, Chubays and Chernomyrdin, rather than an operation planned in advance. SBP guards at the Government House (the White House) claimed that the two aides were leaving the building with \$500,000 in foreign currency and no authorizing property pass or documents.⁷⁸

The SBP and FSB questioned them for several hours, either at the government building or at Moscow FSB headquarters.⁷⁹ One of the aides, Arkadiy Yevstafyev, in a 20 June interview on RTV, said he had been arrested at 5 p.m. Moscow time by the SBP and interrogated until 3 a.m. On 21 June, *Segodnya* specified that Yevstafyev was arrested at 4:15 a.m., while Sergey Lisovskiy was arrested separately at 5:00 a.m., and it said that Lisovskiy was carrying the money. *Segodnya* also reported that, at midnight, Deputy Finance Minister German Kuznetsov arrived at the White House with documents signed by Chernomyrdin, authorizing Lisovskiy to have the money.

Since one of the aides, Yevstafyev, was an official of Chubays's campaign group and the other was at least associated with the campaign, SBP and FSB leaders apparently saw the opportunity of building a corruption case against Chubays and perhaps Chernomyrdin as well. Yevstafyev was a longtime aide and press secretary to Chubays and was linked to Chubays's campaign group, while the other, Lisovskiy,⁸⁰ was a "well-known show business figure" and organizer of a series of big music concerts to promote Yeltsin's candidacy.⁸¹

Tamara Zamyatina wrote in the 21 June 1996 *Izvestiya* that "any scandal involving undocumented and even documented foreign currency, which Lisovskiy and Yevstafyev had taken out of the government building, would cast suspicion on the headquarters' leaders, primarily Chernomyrdin and Chubays," and so could be used "to retrieve the position lost by Soskovets in the election campaign and make him premier after the second round of the election."⁸² Whether the aides actually were carrying the money is in dispute, since, according to Chubays at his 20 June press conference, they

deny having had any such money and Chubays suggested that the money was planted, as part of a “traditional KGB/Soviet-style provocation.”

The two aides were questioned apparently with the idea of finding evidence of wrongdoing by Chernomyrdin and Chubays. NTV President Igor Malashenko said Lisovski told him that FSB interrogators had tried to get from him “any kind of compromising material on the organizers of Boris Yeltsin’s election campaign,” specifically Chernomyrdin and Chubays.⁸³ Yevstafyev in his 20 June interview mentioned comments by his SBP interrogators about the election that suggested hostility toward Yeltsin’s reformist aides. He said his interrogators contended that Yeltsin would win reelection “but not thanks to those who have attached themselves to the president” but thanks to the “real patriots.”⁸⁴

Chubays in his 20 June press conference said that “Korzhakov’s people” conducted the interrogation and used “disgusting and dirty methods” and claimed that the arrests were aimed at the head of the president’s campaign headquarters.⁸⁵ Chubays in his 20 June 1995 NTV interview said the purpose of the arrests was to “demonstrate who rules the roost” and to “intimidate us” in the campaign staff.

Korzhakov and Barsukov later sought to dismiss any idea of a political angle to the arrests. Barsukov said that the reason for the arrests was that the two had attempted to smuggle “a substantial sum of hard currency” out of the White House, and Korzhakov said “there is no political feature to their case, but if people leave the White House with a boxful of hard currency, the police are bound to get suspicious.” He criticized “attempts to stir up the public by presenting the case as politically motivated” and said he had told Lebed to “take it easy.”⁸⁶ Moscow FSB Chief Trofimov denied that the two had been arrested, contending that there had just been a “conversation” conducted “in a civilized form, with tea and coffee,” and that no compromising material was being sought.⁸⁷

The SBP and FSB detention of persons connected to Yeltsin’s campaign staff apparently stemmed from the bitter rivalry between Yeltsin deputies over who was to run the campaign. Yeltsin had designated Soskovets as chief of his campaign headquarters in January⁸⁸ but had replaced him in March when he set up a “Council for the Reelection of Boris Yeltsin,” with himself as nominal chairman. Chernomyrdin, Ilyushin, Filatov, Barsukov, Korzhakov, and others were included as members of the new council, but not Soskovets. Soskovets’s sidelining followed criticism of his handling of the campaign by Filatov and presidential Assistant Georgiy Satarov. Under Yeltsin’s honorary chairmanship, Chernomyrdin and Ilyushin were reportedly actually directing the council.⁸⁹

Meanwhile, Filatov led a campaign group (the All-Russian Movement of Public Support of Boris Yeltsin—ODOPP).⁹⁰ Chubays quietly headed a related but shadowy campaign organization, the creation of which was never announced. In his 20 June press conference, Chubays mentioned that he headed an “analysis group” connected with the campaign headquarters,⁹¹ which prepared strategy. For example, he said the group estimated that turnout would be the key to winning the runoff and therefore pushed for a weekday election date (3 July) instead of the traditional Sunday.

Korzhakov’s bitterness at Soskovets’ ouster—and with it his own reduced influence—erupted at a meeting of the council when Korzhakov told Filatov, Chubays, and Satarov to stop appearing on television.⁹² According to other versions of the exchange, Korzhakov warned Chubays, Filatov, Satarov, and president assistant Aleksandr Livshits to keep their “mugs” off television,⁹³ telling Chubays and Filatov that they “irritate the electorate.”⁹⁴

Chubays, whose campaign aide was one of those arrested, apparently was the first figure to learn of the arrests and played the most outspoken role. As an old enemy of Korzhakov and Soskovets from his time as first deputy premier and reform supervisor and with his aide one of those arrested, he clearly considered himself to be the prime target of the arrests. Chubays spread the word to Chernomyrdin, Lebed, and perhaps Yeltsin. In his 20 June press

conference he explained that he had learned of the arrests three hours after they occurred (8 p.m.) and that within a half hour Chernomyrdin, Lebed, and Yeltsin had been informed.⁹⁵

In his 20 June NTV interview he said he contacted Lebed about 1 a.m. and that Lebed took a strong stand. He also said he phoned Barsukov, who denied knowledge of the arrests. Chubays said that, when he pressed Barsukov for an answer, Barsukov began threatening him and demanding that he come to FSB headquarters.⁹⁶ “Chubays’s people” also sent faxes around midnight to ITAR-TASS about the arrests and apparently notified television channels and radio Ekho Moskvyy as well,⁹⁷ setting off the dramatic television reports of a coup.

The newly appointed Lebed appeared to play into the hands of Chubays in heightening the sense of crisis and turning the situation against Korzhakov. On 18 June 1996, Yeltsin had appointed Lebed as Security Council secretary and presidential assistant for national security in an effort to attract Lebed’s voters in the runoff. Although the full extent of Lebed’s powers was not immediately clear, he was given supervision over all the power ministries, including Korzhakov’s SBP and Barsukov’s FSB.

As the new overseer of the security agencies, Lebed had the right to be informed of any significant arrests by the police. Initially, he took a somewhat alarmed view, probably incited by Chubays’s account of the arrests and caught off-guard by reporters. Someone tipped off reporters to watch for Lebed going to his office about 3:30 a.m., and they caught him on the street at 4:20 a.m. for an impromptu interview.⁹⁸ In his first remarks, he expressed himself sharply, stating that his “first impression” was that “someone is trying to wreck the second round of the presidential election” and declaring, “any mutiny will be quashed ruthlessly.”⁹⁹ Lebed issued a statement that he would not permit any violations of the constitution or laws and would suppress any actions by the power ministries intended to destabilize the country and disrupt the coming elections.¹⁰⁰

Lebed appears to have directly clashed with Korzhakov and Barsukov over the arrests. On 19 June at 3:20 a.m. Moscow time, ORT reported that Lebed had been informed of the arrests several hours earlier and had demanded a report on them from Barsukov and Korzhakov. Chubays in his 20 June NTV interview said Lebed immediately demanded a report from Barsukov but that Barsukov tried to avoid answering the phone. In an interview, Korzhakov complained about the media frenzy and, suggesting that Lebed had been angry about the arrests, said he had told Lebed that “the picture will very soon clear up” and to “take it easy.”¹⁰¹ Korzhakov later complained to reporters that someone was “trying to drag Aleksandr Lebed into this incident.”¹⁰²

Although Lebed himself has not said much about his role in the dispute, Chubays played it up in an apparent effort to make him appear closer to the reformers’ side and to heighten pressure on Korzhakov. In his 20 June press conference, Chubays stated that Lebed had played a key role and displayed “courage” and “decisiveness.” In his 20 June NTV interview, Chubays said that, when he told Lebed what had happened, Lebed took an “unequivocal” position, giving a “cold shower” to the organizers of the detentions and quickly demanding a report from Barsukov.

In his 20 June press conference, Chubays stated that Chernomyrdin had also played a major role in the drama from the start. Chubays said he had phoned Chernomyrdin on the night of 19 June and that Chernomyrdin had “showed himself to be what would be called a real man,” adding that events turned out the way they did “thanks to his position.”¹⁰³ Chernomyrdin was informed of the arrests during the night and had a report by morning. He later said the arrested aides were pressured to testify against him.¹⁰⁴

Chernomyrdin was the first to talk to Yeltsin on 20 June about what to do about Korzhakov, and in that talk he insisted that Soskovets be fired, according to Yeltsin’s Press Secretary Sergey Medvedev.¹⁰⁵ Chernomyrdin was naturally hostile to Korzhakov because of Korzhakov’s past

efforts to undermine him and have him replaced as premier by Soskovets, as well as because of Korzhakov's moves against Chernomyrdin during Yeltsin's October hospitalization. However, in his public statements he did not dramatize the situation, unlike Chubays.

Yeltsin's closest aide other than Korzhakov, First Assistant to the President Ilyushin, played a less visible role, perhaps because he was not part of the reform camp and not one of Korzhakov's prime targets. Nonetheless, Ilyushin had problems with Korzhakov,¹⁰⁶ and as one of the leaders of the election campaign, Ilyushin was involved with demoting Soskovets the previous March, although no one has mentioned him advising Yeltsin to oust Korzhakov or Soskovets on 20 June. He publicly criticized the arrest of the two aides, calling it "detrimental to the president's election campaign."¹⁰⁷

Media Plays Up Arrests

The media—especially television—played a key role by reporting the arrests and developing a crisis atmosphere by accusing Korzhakov and Barsukov of attempting a virtual coup. The media were initially informed of the arrests by faxes and phone calls around midnight from "Chubays's people."¹⁰⁸ Starting soon after midnight, television began reporting the arrests and creating a crisis atmosphere by staying on the air during the night and carrying special bulletins about the arrests. For example, in the first report of the arrests, at 1:20 a.m., NTV's Yevgeniy Kiselev broke into NTV programming to report the arrests and characterize them as "the first step in implementing a scenario for canceling the second round of the presidential election"¹⁰⁹ and to declare that the "country is on the brink of political catastrophe."¹¹⁰

The pressure from television played a key role and apparently forced the release of the two detainees. NTV Chairman Malashenko said Lisovski told him that, as soon as NTV and ORT began reporting the arrests, the two were released.¹¹¹ In his press conference, Chubays said that the television reports had played a crucial role and that as soon as the

first report appeared on television, the interrogators "suddenly turned gentle" and stressed that they did not want any "televised scandal."¹¹²

Influences on Yeltsin's Decision

The dispute came to a head on Thursday morning (20 June), as Chubays and Chernomyrdin managed to raise the stakes so high that Yeltsin decided to fire his three trusted aides. The major input into the decision to fire Korzhakov, Barsukov, and Soskovets reportedly came from Chernomyrdin and Chubays. Medvedev on 20 June said that Yeltsin first met with Chernomyrdin then discussed the changes at a Thursday morning Security Council session.¹¹³ Following that, he held successive meetings with Korzhakov and then with Chubays before making his decision. Medvedev also specified that Chernomyrdin urged Yeltsin to fire Soskovets, blaming him for "serious mistakes" in running industry and defense industry conversion.¹¹⁴

Chubays in a later NTV interview said that in his talk with Yeltsin the president had asked him what happened, who "instigated" the arrests, and why.¹¹⁵ Chubays had appeared ready to force the issue by scheduling a press conference for 10:30 a.m. with Yevstafyev and NTV Chairman Malashenko on the theme "An Attempt To Disrupt Boris Yeltsin's Election Campaign." This press conference was only postponed when Yeltsin agreed to meet Chubays at noon. Yeltsin then announced the dismissals at about 12:30 p.m., after which Chubays held his press conference.

Yeltsin's decision appears to have been based more on considerations of power and concern about Korzhakov's possibly jeopardizing his reelection than on possible legal abuses in the arrests. He appeared uncertain over whether the arrests were a serious matter, saying that "I don't know the details, but judging from what senior officials told me, it was a purely technical affair"¹¹⁶ and adding that the aides had "violated the pass rules and were detained for this reason."¹¹⁷ Medvedev quoted Yeltsin as saying that the dismissals were not linked to the arrests.¹¹⁸

Nonetheless, the dispute apparently convinced Yeltsin that it was time to dump Korzhakov and his allies. Yeltsin had shown irritation with Korzhakov recently for publicly proposing postponement of the election and had ordered him to stop meddling in politics. Although Soskovets was apparently not involved in arresting the campaign aides, he was dismissed also, apparently because of his close maneuverings with Korzhakov against Chernomyrdin.

When Yeltsin announced his decision to remove Soskovets, Barsukov, and Korzhakov to television cameras, he first characterized it as a “renewal” of his team, but then showed his irritation at having to repeatedly defend Korzhakov and the others. He complained, “I am always being reproached for Barsukov, Korzhakov, Soskovets,” and asked, “should the president work for them?” He asserted, “it has never happened that I worked by Korzhakov’s suggestions”¹¹⁹ and added that the “power structures need to be replaced; they took too much on themselves and gave back too little.”¹²⁰

Despite his initial anti-Korzhakov statements during the night—uttered when he was caught off guard by reporters—Lebed seemed to play a more conciliatory role than Chubays and Chernomyrdin, playing down the conflict, not publicly attacking Korzhakov and Barsukov, and even claiming to have tried to reconcile the two sides.

Initially after the Security Council meeting, Lebed denied that the council discussed the arrests,¹²¹ saying it had discussed measures against crime and corruption.¹²² He called the arrests only a “misunderstanding”¹²³ and turned back questions about his role in ending the arrests, stating “this murky story does not interest me. This is a question for investigation by the prosecutor and FSB.”¹²⁴

He claimed that he had tried to reconcile the sides, mentioning “I almost reconciled the participants of the well-known conflict which took place in the early hours of Thursday.”¹²⁵ After Yeltsin dismissed the hardliners, Lebed followed Yeltsin’s lead in downplaying the dismissals. Like Yeltsin, he characterized the firings as just a changing of the

guard rather than part of a political struggle. New on the job and unfamiliar with the bureaucratic infighting, Lebed refused to comment on the factional struggle, saying he is “still a young party big shot and has not figured out the tricks.”¹²⁶

Reformers’ Versions

Chubays, Filatov, and Satarov were less restrained than Lebed, accusing Korzhakov, Barsukov, and Soskovets of forming a hardline faction, attempting a coup, and trying to cancel the election, and they also boosted Lebed’s role in resisting them.

Chubays described the events in detail during his 1:30 p.m. press conference on 20 June, characterizing the incident as a struggle between those who wanted to use force and avert elections—naming Korzhakov, Barsukov, and Soskovets—and those who wanted to carry through with elections. He said Yeltsin’s 16 June election victory “made almost pointless the attempts to direct the situation to strong-arm solutions” and claimed that with Lebed’s appointment the alleged conspirators had lost their “last hope.”¹²⁷ He argued that the events had constituted a “coup attempt”¹²⁸ and called Soskovets the “spiritual father” of the Korzhakov group.¹²⁹

Filatov—another bitter foe of Korzhakov—also dramatized the situation, calling the events a scandal and accusing Korzhakov and Barsukov of “constantly interfering in the work of the election council, even though the president already in May had advised Korzhakov not to intrude into politics.” He claimed Korzhakov had been frightened by Lebed’s “increased influence” and accused Korzhakov of actively helping to defeat St. Petersburg Mayor Anatoliy Sobchak’s reelection bid.¹³⁰

Satarov said that the influence of Korzhakov and Barsukov “dwindled” as Yeltsin’s popularity rose, and they decided to “seize the initiative” from Chernomyrdin and others and prevent Lebed from consolidating his position. Satarov said, “it has become easier to breathe” now that Korzhakov is gone.¹³¹

Despite his success in having Korzhakov and his allies dismissed, Chubays's bold statements, as well as his pressure on Yeltsin to fire Korzhakov, apparently angered the president. On 26 June, *Segodnya* reported that Yeltsin was extremely unhappy over Chubays's public statements about the events and had decided to limit Chubays's campaign role or possibly even dismiss him. Korzhakov meanwhile called Chubays's press conference statements "100-percent lies."¹³²

Reformers took advantage of Korzhakov's ill-fated move to achieve results that they had long been seeking—to Yeltsin's hardline and ambitious bodyguard and confidant, who felt free to interfere in all sorts of political and economic decisions. Korzhakov lost direct control over his police forces (the SBP), which he used to intimidate others and exercise power. Lebed's actions in this crisis—coming before he had learned his way around Yeltsin's staff—made it difficult to clearly define Lebed's role and political inclinations, but, in this case, reformers were able to effectively get Lebed on their side in the bureaucratic struggle for power.

Kovalev Named FSB Chief

When dismissed on 20 June 1996, Mikhail Barsukov had served as FSB head for less than a year. Yeltsin named a deputy director of the Federal Security Service (FSB), Col. Gen. Nikolai Kovalev, as its new acting chief. Kovalev's intelligence service activity began in 1974 with his entrance in the KGB, where he joined the Fifth Directorate, which dealt with ideological questions and the questions related to dissidents. He served for two years in Afghanistan and later worked in the Moscow and Moscow Oblast branches of the FSB before being made deputy director with responsibility for the Investigations Directorate, Directorate for Economic Counterintelligence, and Operational Reconnaissance Directorate. After his nomination to the FSB, Kovalev told the news media that he saw the emphasis of his activities in the economic security of Russia and in the fight against corruption. In addition, he promised to focus on measures to respond to increasing activities of foreign intelligence services in Russia.

In addition, Yeltsin simply put FSO¹³³ Director Yuriy Krapivin, a Korzhakov-Barsukov deputy, in charge of Korzhakov's SBP.

In 1995 and 1996 the FSB reported that a total of about 400 foreign intelligence officers were uncovered working in Russia and put under FSB surveillance. The FSB also claimed it neutralized the activity of 39 foreign intelligence agents who were Russian citizens and stopped more than 100 attempts by Russian citizens to pass secret information to foreigners. A spate of articles in the national and provincial press by FSB spokesmen boasted the service's role in protecting the state from foreign subversion. FSB Director Kovalev said, "There has never been such a number of spies arrested by us since the time when German agents were sent in during the years of World War II."

One of the cases was that of US Army Captain Jason Lynch, who the FSB accused of conducting intelligence activities. The US State Department refuted the Russian charges on 11 August 1995, adding that Lynch, a West Point instructor, left Russia as originally scheduled following an official Russian protest that he had engaged in intelligence activities. According to the State Department spokesperson, "those charges are absolutely unfounded. Captain Lynch was engaged in an environmental study of radiological contamination along the Yenisey River in Eastern Siberia at the invitation of the Institute of Biophysics. All of Captain Lynch's activities in Russia were under the direction of and in conjunction with his Russian hosts."¹³⁴

The Yeltsin administration in October 1997 and January 1998 made broad new categories of environmentally related information subject to secret classification. These include defense-related meteorological, geological, and cartographic work; the surveying and production of precious minerals; and the use of land and water by security services. The Yeltsin administration also instituted policies mandating that all information pertaining to military nuclear facilities be classified state secrets in response to damaging revelations about environmental problems by former military officers and others.

The FSB arrested individuals on false pretexts for expressing views critical of the government, including harsh criticism of the security services. The FSB also targeted national security and environmental researchers. The Russian press indicated those Russian citizens interested in military issues or military-industrial polluters became FSB targets.

For example, the FSB arrested Vladimir Petrenko, a former military officer in Saratov Oblast, in mid-1995 following his research into the danger posed by military chemical warfare stockpiles. He was held in pretrial confinement for seven months on what Amnesty International and Russian human rights observers believe is a trumped-up charge of assault.

A few months later, the FSB accused the Norwegian environmental Bellona Foundation of collecting state secrets on Russia's Northern Fleet in October 1995. The group had gathered material for a second report on the Fleet's nuclear waste. The FSB raided the group's Murmansk office; confiscated all material on the Fleet's nuclear waste sites, as well as computers and video cameras; interrogated researchers working on the study; and searched many of their homes. Others cooperating with Bellona in Murmansk, St. Petersburg, and Severodvinsk also were interrogated and subject to apartment searches.

Viktor Orekhov, a former KGB officer who assisted dissidents under the Soviet regime, was arrested in 1995 and charged with illegally possessing a firearm soon after he made critical comments in an article about his former boss, who was then serving as FSB chief of intelligence for the Moscow region. Within weeks Orekhov was tried, convicted, and sentenced to three years in prison. His sentence was later reduced to one year. Orekhov claimed the FSB targeted him for retribution because of his involvement in human rights, and he cited the speed at which he was tried and sentenced in the usually slow Russian court system. The FSB's influence and interest in the case were extensively reported in the domestic and foreign press.

On 6 February 1996, the FSB arrested Aleksandr Nikitin in his home in St. Petersburg and charged him with high treason through espionage and divulging of state secrets. FSB officials justified their actions by claiming he was involved with the Bellona report on nuclear-hazardous objects of the Russian Northern fleet, which contained state secrets. In addition, the FSB charged that Nikitin used credentials that he had not returned on his discharge from military service, appealed to a colleague and obtained access to information subject to state secrecy, and, for the same purpose, forged credentials to penetrate a closed zone. (See below for details on the Nikitin Case.)

In December 1996, Nikolay Shchur, chairman of the Snezhinskiy Ecological Fund, was held in pretrial confinement for six months following his survey of military pollution near Chelyabinsk.

According to June 1998 Reuters reporting, President Yeltsin took action to step up the Russian counterintelligence service's efforts to protect the nation's economic, constitutional, and computer security. The Kremlin said that at the beginning of 1988 it became concerned about growing foreign espionage activities against Russia, including the use of computer networks.

Some senior officials expressed concern about the spread of the Internet in Russia, saying that computer hacking and computer-related crimes pose a serious threat to national security. But FAPSI said its lines are impregnable to hacking due to high-tech, antibugging devices and top-secret data encryption. FAPSI is now marketing some of its voice and data encryption technologies for common use.

FAPSI further said foreign secret services were massively intruding "with the aim of influencing state structures, banks, industrial enterprises, scientific organizations and mass media." Senior intelligence officials frequently denounced suspected Western interference in Russian domestic affairs. The concern was so great that Yeltsin discussed the issue with FSB head Kovalyov.

Kovalev Out—Putin In

For reasons not totally clear, Kovalev was fired. On 25 July 1998, Yeltsin nominated Vladimir Putin as FSB Director. The Russian and foreign media knew very little about the new boss of the FBS and latched on to his past in the KGB and his less than cuddly media image. Putin became a permanent member of the Security Council at the beginning of October 1998, and at the end of March 1999, the Secretary of the Council. His position as FSB Director gave him also a seat on the Interdepartmental State Defense Orders Commission.

The Russian press floated various theories about why the Kremlin replaced Kovalev with Putin, a Yeltsin loyalist who reportedly had ties to Chubays.¹³⁵ The reports and commentaries, however, tended to view the “reliable” Putin’s appointment as an effort to ensure the FSB’s loyalty in the event of a socioeconomic crisis or some other crisis scenario, such as moves against Yeltsin by the Duma or others, or a Yeltsin dissolution of the Duma.

As early as 22 July, the Boris Berezovskiy—financed *Nezavisimaya Gazeta* implied that Yeltsin wanted a more dependable figure in control of a key “power department” in the event of a political crisis. The newspaper maintained that the Kremlin was “unable to forecast” how Kovalev would behave if the Duma impeached Yeltsin.

The newspaper later maintained that Kovalev had refused to help the Kremlin prepare the ground for a Yeltsin third term by conducting “large scale political investigations” of Yeltsin’s 2000 presidential rivals.¹³⁶ On the other hand, *Russkiy Telegraf* and *Komsomolskaya Pravda*, controlled by Berezovskiy rival Vladimir Potanin, saw Kovalev’s removal as politically motivated.

In the 28 June issue, Yelena Tregubova wrote that Yeltsin had found a “strong” “Chubays man” in Putin, then chief of the president’s Main Control Administration, to “gather the power ministers into a single strike force” and “prepare for the fall season.” Putin would be a reliable FSB chief

who would oppose an anticipated “fall offensive” by “hard-line reds,” “some regional leaders,” and “malcontent oligarchs.” Igor Chernak, writing in *Komsomolskaya Pravda*, maintained that Yeltsin saw Kovalev as “unreliable” in view of the forecast of a “hot fall” and “talk” of coup plots.¹³⁷

Communist (CPRF) Duma opposition leader Gennadiy Zyuganov expressed concern over Kovalev’s replacement by Putin. Zyuganov claimed that the change might signal the beginning of a “creeping coup.”¹³⁸

Putin’s appointment was the latest by Yeltsin to return the intelligence agency’s clout by tapping into the KGB’s experience of imposing control and gathering information. Putin kept his FSB job until 9 August 1999 when Yeltsin made him Acting Prime Minister. His FSB position was given to Nikolai P. Patrushev.

During a 25 July 2000 speech marking the promotion of officers during a ceremony in the Kremlin, Prime Minister Putin said that he was against reuniting the country’s intelligence services into a single unit modeled on the Soviet-era KGB. “We do not need this,” the president said, “but each of the services should be close enough to the other to feel its shoulders.”¹³⁹

While dismissing the idea of the restoration of the old Soviet State, it is hard not to notice what was happening in Moscow. In early March 2000, Alexander Korzhakov, a prominent member of the Russian parliament and former Yeltsin top adviser, called for the KGB’s restoration. Korzhakov said that those opposed to the KGB “now admit that the dissolution of the agency gained us nothing . . . It’s time for us to unite all our secret services into a tight fist and strike at those who are preventing us from living normally. Russia needs a KGB. Let’s stop being coy about it.”

During Putin’s visit to India in October 2000, the FSB signed an accord with the Indian Ministry of Internal Affairs on “the mutual protection of classified documents,” according to the Russian Government’s press office on 3 October. The

accord adopts the third agency rules, which requires both services not to provide any secret data to another service. It also makes Russian secrets Indian secrets, thereby potentially making an Indian citizen a criminal in his/her country if he/she has unauthorized access to Russian documents.

Under President Putin: FSB Supplants the “Old Guard”

The Moscow Institute of Political Research Director Sergei Markov said that President Putin views the two kinds of oligarchs in Russia as separate and distinct. The “old” oligarchs, who include Berezovsky, Potanin, Mikhail Khodorkovskii, Mikhail Fridman, Petr Aven, Rem Vyakhirev, and Vakhit Alekperov, became rich from sweetheart deals with the former government. Putin viewed them as political opponents who must be destroyed because of their political skills.¹⁴⁰

Taking a page from Soviet Communist Party founder Vladimir Lenin who used the secret police to arrest rich Soviet industrialists and businessmen, Putin made legal moves against his country’s industrial titans. Vyacheslav Soltaganov, chief of the Federal Service of Tax Police (FSNP), reported to Putin regularly on the FSNP’s tax evasion and money-laundering investigations against them. After one reported meeting, the FSNP, the office of the procurator-general, and FSB redoubled their investigative efforts against firms connected with Potanin, Alekperov, and Berezovskiy. In addition, they intensified their pressure on Vladimir Gusinsky and his media empire.

The second, or “new,” oligarchs included Roman Abramovich, Aleksandr Mamut, Oleg Deripaska, Sergei Pugachev, and many lesser-known businessmen. Putin viewed them as potential allies because he believed they would easily fall in line, but this has not been the case. These oligarchs came under the same scrutiny by the FSB as the “old ones.” Sibneft head and leading Yeltsin-era oligarch Abramovich¹⁴¹ was summoned to a Moscow police station for questioning about tax evasion. For some media commentators, these

moves suggested that Putin finally begun a quiet but sweeping purge of the corrupt officials and businessmen he inherited from Yeltsin.

Although Sibneft was losing its position as “one of the main fuel suppliers,” the real target behind the targeting of Abramovich was Deputy Defense Minister General-Colonel Aleksandr Kosovan, a “little known . . . grey cardinal” who, earlier press reports charged, “stands in one rank with Abramovich” and other oligarchs. In charge of troop housing construction and billeting since 1992, Kosovan was said to be “the main military oligarch” who, among other malfeasance, fictively wrote off as spilled or lost “one half” of the fuel and lubrication materials he bought for the army. He then sold the “spillage” on the open market, splitting proceeds with his suppliers for the military.¹⁴² The media suggested that Abramovich was being pressured to help the Kremlin deprive his onetime ally and partner Berezovskiy of Sibneft funds.¹⁴³

Putin’s Second Year

Putin took further action as he began his second year as President. He made a number of appointments, which some Russia media interpreted as the start of the long-awaited and long-promised “purging of the oligarchs.” Others, however, considered Putin’s moves feeble and meandering. They saw the shakeups in the government and in government-owned businesses as merely an extension of the old interoligarch battles. The only difference being that younger pretenders were not fighting for spoils. While some skeptics saw Putin’s appointments as further proof of his perceived weakness, many others noted the many FSB and KGB alumni among the new faces and argued that Putin’s “house-cleaning” would end with the FSB in control of large parts of Russia’s economy.

Since mid-May 2001, Putin removed Yuriy Petrov from the scandal-ridden State Investment Corporation (Gosinkor),¹⁴⁴ eased longtime head Vyakhirev out of Gazprom, and replaced the oligarch-linked Minister of Natural Resources

Boris Yatskevich.¹⁴⁵ Putin appointed Igor Yusufov as the minister of energy, thereby filling a vacancy that had existed since the president fired Aleksandr Gavrin in February 2001 for poor performance. A graduate of the Academy of Foreign Trade, Yusufov previously worked in the Russian trade mission in Cuba, the Committee for the Protection of Russian Economic Interests, and the Ministry of Industry. He also worked in the state reserves committee, which has close ties to the FBS.

Russians who had been speculating about large-scale cabinet shakeups for a year or more found the appointments of Yusufov and Vitaliy Artyukhov as Minister of Natural Resources to be insignificant and disappointing.

Artyukhov has had a checkered governmental career, most of it in the Ministry of Transport, where he was in charge of highway construction. In 1996 he was made head of the State Tax Service, with Deputy Prime Minister status, but soon was returned to the Ministry of Transport as Deputy Minister.¹⁴⁶ Artyukhov's son, Vadim, is called "one of the main Kasyanovites" (shorthand for supporters of Prime Minister Mikhail Kasyanov, frequently linked to "old guard" oligarchs and officials of clouded reputation) and has been accused of sharing "invisible business ties" to Abramovich and Yeltsin-era court banker Mamut.¹⁴⁷

Yusufov is reported to have "an extremely scandalous reputation."¹⁴⁸ He is from an "extremely rich clan of Tats (mountain Jews) who are always suspected of buying their high positions." Yusufov is said to have bribed two deputies of then-Prime Minister Sergey Kiriyenko—Viktor Khristenko and Boris Fedorov—in appointing him Deputy Head of the Russian Agency for State Reserves (Goskomreserv), the agency of which he had become General Director before appointment as Energy Minister.¹⁴⁹

Prior to that, Yusufov was Deputy Minister of Industry in 1996-1997, with responsibility for the gold and diamond sector. At that time, Yusufov was suspected of collaborating in the "illegal and semi-legal export" of raw diamonds "to Israel and Belgium."¹⁵⁰ Yusufov is called a

"close acquaintance" of Deputy Finance Minister and head of the State Fund for Precious Metals and Precious Stones (Gokhran) Valeriy Rudakov, as well as of Israeli diamond billionaire Lev Levayev,¹⁵¹ both reputed to be allies of Abramovich.

Mikhail Leontyev, a commentator on ORT television who is famed for his caustic editorials, dismissed the latest ministerial appointments as illustrating that "the new dominant principle of our government's personnel policy is to appoint amateurs to ministerial posts, because amateurs are thought to steal less than professionals."¹⁵²

While Putin's appointments maintained the outward appearance of the offsetting "checks and balances" that Yeltsin had employed to play rival factions off against one another,¹⁵³ in fact, Putin was conceding less important posts to entrenched interests and putting his own people into key positions. Thus the "old guard" was "nevertheless being squeezed out, albeit very slowly and 'without revolutions'—just as the president promised, in fact."¹⁵⁴ Other commentators, however, explained the pattern of dismissals and appointments in the context of a larger fight by political and business figures from St. Petersburg to expand their own turf by capitalizing on Putin's ties to the region.

Putin's appointments of Artyukhov and Yusufov were deemed unimportant tactical concessions to the "old guard." The real control of these administrative empires was under "Petersburg appointees" Aleksey Poryadkin, First Deputy Minister of Natural Resources for Forests and Wood Products, and Deputy Minister of Natural Resources Yelena Katàyeva, a classmate of Putin from law school who oversees the legal department, including development and site licensing.¹⁵⁵

The appointment of Aleksei Miller—a Putin associate since St. Petersburg days—to head Gazprom was another sign that Putin "has begun to form his own team," with "the FSB, the SVR, [electricity monopoly] RAO YeES, the oil industry, the presidential administration, the military-industrial complex, and space" up next to be reformed.¹⁵⁶ The proadministration newspaper *Rossiyskaya Gazeta*

made the same argument that “the command of the country’s main raw-materials bastions has been replaced” because “the country’s leadership” wishes to “secure a greater return from the extraction industries.”¹⁵⁷ Even more dramatically, Moskovskiy Komsomolets, prone to yellow journalism, declared “the ‘taking’ of Gazprom is no less significant than the taking of the Bastille by the Parisians in 1789.”¹⁵⁸

According to journalist Yelena Kiseleva, there are now so many “Petersburgers” in the government that people “in the coulisses of power” have begun to joke that the Kremlin sends representatives to meet the Red Arrow train as it arrives each morning from St. Petersburg, asking the “pale, clumsy youths” who stumble out whether they are Petersburgers and, if so, whether they would like to work in the government.¹⁵⁹ Other “Petersburg appointees” whom the media have identified include Deputy Minister of Finance Yuriy Lvov, in charge of “financial intelligence-gathering in Russia;” Sergey Vyazalov, named head of Gosznak, the government’s mint; Aleksandr Vasilyev, named head of the Moscow tax police; deputy Director of the Federal Tax Police Sergey Verevkin-Rokhalskiy; “head of the [tax police] operative division” Vladimir Vorozhtsov; and Vladimir Chernov, new head of Gosinkor.¹⁶⁰

Some media have begun to note that, in addition to their connections through St. Petersburg, many of Putin’s appointments also are tied in one way or another to the KGB or its successor, the FSB.

Chernov, for example, not only served in the “Soviet-Finnish Trade Mission” when Putin was head of St. Petersburg Committee for Foreign Trade Relations, but is also rumored to have served in the “foreign intelligence directorate” of the KGB with Defense Minister Sergei Ivanov. Ivanov is said to have lobbied for Chernov’s appointment, suggesting a concerted effort by the security services to control potentially lucrative Gosinkor.¹⁶¹ Another report said, however, it was Chernov himself who “actively sought this position through the presidential administration.”¹⁶²

The Russian Agency of Political News characterized Chernov’s appointment to mean that Gosinkor “had now passed into the direct control of the special services FSB.”¹⁶³ It was asserted that Deputy Director of the FSB Yuriy Zaostrovtssev—“an experienced warrior against illegal financial operations” because of his “recent experience with similar questions in the [Gosinkor-affiliated] Guta-Bank”—would shortly be named First Deputy Chairman of the Central Bank.¹⁶⁴

Another article predicted that an important financial source would also soon fall to the FSB, which is pushing to install “KGB colonel Aleksandr Kozlov” as head of the State Repository for Precious Stones and Precious Metals (Gokhran), a position Kozlov had held “in the early 1990s” when this was Gokhran.¹⁶⁵

According to another report, the Deputy Director of Economic Security in the FSB, “Colonel Zhukov, has already been seconded” to work in Gazprom and may “soon be joined” by a senior colleague, “General Nurgaliyev,” who may become Deputy Director of Gazprom.¹⁶⁶

Putin appointed former SVR chief Vyacheslav Trubnikov first deputy of the Minister of Foreign Affairs and the presidential envoy in the Commonwealth of Independent States (CIS) countries in June 2000.¹⁶⁷ According to Russian media, Trubnikov’s appointment suggested a tougher Moscow line toward the CIS and Baltic countries. At the same time, it signaled the comeback of Primakov and his team to the foreign policy arena as Primakov joined Putin’s administration as the coordinator of Russia-Moldova settlement.

Trubnikov’s appointment apparently paid off. At the CIS summit in Moscow—21-23 June 2000—these countries supported Putin’s request to establish “a joint anti-terrorist center.” The center, to be located in Moscow and funded by the Russian Government, was to be headed by FSB Gen. Boris Mylnikov.¹⁶⁸ Although the center is to coordinate antiterrorist efforts across the CIS, its responsibilities in this area will be extremely limited since it would have no combat units under its direct control.

The center is viewed by many as a means by which Moscow wants to try to regenerate the CIS by bringing into play the threat of a common enemy and to gain support for Russian policies in Chechnya. The Moscow endeavor may be doomed to failure because CIS members confront different security challenges and because there is no consensus on Chechnya.

On 7 August 2000, Putin named career KGB officer Yuriy Demin first deputy minister of justice. Demin joined the KGB in the 1970s. From 1992 to 1997 he served as the chief of the FSB's legal service. In 1997 he became chief military prosecutor for the Russian Federation. Although functionally a deputy of former Prosecutor-General Yuriy Skuratov, Demin supported the Kremlin in its clash with Skuratov.

In a possible move to counteract criticism of Putin's moves, former KGB chief of foreign intelligence Leonid Shebarshin praised Putin's use of former KGB officers in his administration as "both natural and reasonable." He noted that many of them had already proved their value in service to Russia. He also commented that both American and British governments had badly miscalculated in thinking that Russian counterintelligence is now "dead." The cases of Platon Obukhov and Edmund Pope, he said, "show just how wrong they have been."¹⁶⁹

Prime Minister Kasyanov appointed Colonel-General Aleksei Shcherbakov to be first deputy communications minister, making him responsible for controlling the country's telecommunications infrastructure.¹⁷⁰ A KGB veteran, Shcherbakov had been the first deputy of the SVR. His appointment was another sign that Leonid Reiman, the communications minister, was turning his ministry into a "special service" for the Kremlin.¹⁷¹ Earlier this year, Reiman authorized the introduction of government monitoring of telecommunications, known as SORM, and allowed the FSB to have anonymous access to the files of users.

Putin appointed SVR veteran Mikhail Dmitriev as the Defense Ministry official responsible for the rearmament of the country's defense forces and also for the export of weapons and military

technology.¹⁷² Until August 2000, Lieutenant-General Dmitriev directed the SVR's analytic information directorate.¹⁷³ His appointment followed the consolidation of the Rosoboronprom under another SVR veteran, Andrei Belyaninov. Their appointments gave Putin direct control over these two key areas.

On 26 March 2001, Putin announced senior personnel changes at three key security agencies: the Security Council, the Defense Ministry, and the Interior Ministry. Sergei Ivanov, who had been in charge of the Security Council, became defense minister. Vladimir Rushailo, who had been at Interior, replaced Ivanov at the Security Council, and Duma Unity head Boris Gryzlov took over at Interior.

The shift of Ivanov to the Defense Ministry in no way reduced his broader security role. Rather, it gave him a new bureaucracy to support his policy ideas. One indication of that were Ivanov's plans to transform the Defense Ministry's 10th Chief Administration from a body supervising defense treaties and representations into a more general strategic planning center. The revamped administration was renamed the Administration for Military Policy. SVR General Dmitriev would head its International Relations department.¹⁷⁴

Putin appointed two members of the so-called St. Petersburg Chekist gang to help new Interior Minister Gryzlov. The former chief of the FSB Personnel Department, Col. Gen. Yevgeniy Soloviev, became head of the ministry's Department of Cadres and Organizational Work, and the former head of the St. Petersburg Special Procuracy for State Security Matters, Vitaliy Merzlyakov, was installed as the head of the ministry's Investigative Committee. In addition, yet another deputy minister, Vladimir Vasiliev, an Interior Ministry functionary who was ousted by former Interior Minister Rushailo, joined them.

It did not take long before these FSB generals effectively took over the Interior Ministry, despite the traditional mistrust between the police and the security organs.¹⁷⁵ It was suggested that this was in many ways a good step because the FSB was

significantly less corrupt than the Interior Ministry has been. But one danger noted was the imported FSB officers might assume total control of the Interior Ministry, and their actions there might become a model for the takeover by the security agencies of other bodies.

Summing up recent appointments, commentator Gennadiy Vasiliyev, writing in the Krasnoyarsk newspaper *Komok*, described Putin as “actively and methodically” moving in “two directions” in order “to change the existing political reality within the country, or more precisely, to create a parallel reality,” by drawing Putin’s “Petersburg comrades . . . more insistently into the political orbit” and by strengthening his power “in the power ministries (to be precise, by [placing] FSB people [there]).”¹⁷⁶

However, claims that Energy Minister Yusufov is also a “rank-and-file FSB” agent suggested that the FSB’s movement into finance and industry—if it is taking place—is not monolithic, or necessarily a strengthening of Putin’s hand. Neither should it be assumed that Putin is an automatic and uncritical supporter of the intelligence services.¹⁷⁷

Speaking to American journalists after his meeting with President Bush, Putin said “both . . . [the Russian and US special services] do a poor job. They do not do anything interesting. They only get in the way.”¹⁷⁸

Changes in the FSB

In May 1997, President Yeltsin signed an edict reorganizing the FSB. According to this document, five departments were introduced in replacement of the existing directorates and services—there were formerly 34 directorates. They were transformed into departments to enhance manageability. According to news reports, within a few months thereafter, the SVR, the border guards, and FAPSI were possibly expected to be cojoined with the FSB—restoring the KGB almost in full—but this did not occur.

After Yeltsin appointed Putin as Prime Minister, he named Patrushev to be FSB chief. Patrushev’s Deputy Director was Colonel General Kovalev—former FSB chief previously ousted by Yeltsin—who was now responsible for the Investigations Directorate, Directorate for Economic Counterintelligence, and Operational Reconnaissance Directorate.

In 1992 the FSB Investigations Directorate was abolished, but in 1995 it was reestablished. The unit takes an active part in combating illegal trafficking in weapons and drugs, corruption, and crimes in the sphere of the economy and organized crime. In 1995 it had more than 1,000 ongoing cases under investigation.

In July 2000, Gen. Col. Aleksandr Tsarenko, the chief of Moscow’s FSB division, was removed and replaced by Valentin Vlasov, the chief of the Moscow FSB Counterintelligence Department.¹⁷⁹ The newspaper believes that Tsarenko was replaced because of his close ties to Moscow mayor Yuriy Luzhkov.

President Putin named Lt. Gen. Sergei Smirnov to replace Aleksandr Grigoriev as head of the St. Petersburg branch of the FSB. Apparently there was a conflict between Grigoriev and another Putin loyalist, Viktor Cherkesov, who is the presidential envoy in the Northwest Federal District. Grigoriev evidently angered Cherkesov because of the FSB’s investigation of the latter’s ties to the Tambov organized crime group. Grigoriev had also expressed skepticism about charges that the former deputy head of the city council, Yuri Shutov, was involved in organizing contract murders. Shutov fell from favor and was arrested after Putin, then FSB director, secretly visited Switzerland in 1999 to cover up Kremlin corruption cases.¹⁸⁰

Under the revised law on Russian foreign intelligence of January 1996, the FSB is also authorized to work outside Russia in certain target areas in cooperation with the Russian foreign intelligence services. The FSB is also seeking expanded cooperation with the intelligence and secret services of the other former Soviet republics.

In September 1996 the managers of most CIS secret services initiated an information system for their managers of the security organs and special services to improve the communication between the involved secret services. A central data bank was established in September 1996 at the FSB, which serves to support the fight against organized crime.

Returning to Yesteryear

During the Edmund Pope trial, an FSB officer approached Andrei Andrusenko, one of Pope's Russian lawyers in the corridor outside the courtroom. Andrusenko had previously said he was under physical surveillance and that his mobile telephone was probably tapped. The FSB officer warned him to be careful. "You lawyers need to know," he said, according to Andrusenko, "the spy will sooner or later go, but you remain in this country, and it's not known who will be next on trial." The veiled threat is an indication of "what many Russian specialists say has been the growing influence and prominence of the security services under President Vladimir Putin . . ." ¹⁸¹

FSB and the Media

On 11 May 2000, the Interior Ministry's Main Directorate for Fighting Economic Crime, the Prosecutor-General's Office, and the tax police raided the Moscow offices of Gusinsky's Media-MOST Group to carry out a search. The search was part of a criminal investigation into former Finance Ministry officials suspected of abuse of office. Media-MOST denounced the action as one of "lawlessness" that was linked to recent reporting by its media outlets on government corruption.

In an article dated 12 May, entitled "Machine Guns in the President's Press Service," "Segodnya" claims that the Media-MOST Group was preparing a series of articles on corrupt high-level law enforcement officials, including Deputy General-Procurator Sabir Kekhlerov and FSB Deputy Director Zaostrovtssev, who also heads

its department for economic counterespionage. As part of its investigation, "Segodnya" claims it sent letters of inquiry to these officials. Instead of responding to the journalist's questions, these officials instead decided to send armed masked men to raid the Media-MOST offices. According to "Segodnya" it was Kekhlerov who signed the order to initiate criminal charges, and it was Zaostrovtssev who supervised the raid. ¹⁸²

In a letter dated 12 May to President Putin, the Committee to Protect Journalists (CPJ) said that the action against Media-MOST, coming only four days after his inauguration, "raises serious questions about his commitment to a free and independent press." The CPJ also pointed to contradictory explanations (financial irregularities, criminal investigation, and illegal eavesdropping) of the raid given by officials from various government agencies. ¹⁸³

In an interview with ITAR-TASS on 11 May, FSB spokesman Zdanovich denounced criticism directed against his agency over the Media-MOST raid. He said, "suggestions that the case was 'political' and represented an attempt 'to put pressure on the mass media' has nothing to do with what is really taking place." Zdanovich insisted that the investigation concerned violations of tax laws. Meanwhile, the law enforcement officers told Interfax that they discovered unauthorized eavesdropping equipment in the Media-MOST offices. ¹⁸⁴

The mounting criticism of the raid on Media-MOST prompted a response from the presidential press service. It announced that Putin is "firmly convinced that freedom of speech and freedom of the media are immutable values" but added that, with regard to criminal investigations, "all are equal before the law no matter what business they are in."

The Secretariat of the Union of Journalists published a statement appealing to Putin to counter the unconstitutional actions of the FSB. ¹⁸⁵ The statement also expressed a lack of confidence in the leadership of Media Minister Mikhail Lesin, who "has done nothing to strengthen the freedoms of the

media.” The previous day, Lesin said “that there are no grounds to believe that federal powers are trying to put pressure on the media and that the raid on the Media-MOST Group will not affect the operation of that holding company’s media organs.”¹⁸⁶

On 15 May, Media-MOST Group accused the FSB of manufacturing incriminating evidence: “The use of open disinformation, falsification and fraud by government-controlled media and law-enforcement officials show such methods are becoming state policy.” Russia’s prosecutor-general, however, said the search was justified and was aimed at finding evidence of eavesdropping by Media-MOST’s security service. Deputy Prosecutor-General Vasilii Kolmogorov said, “claims the media are coming under pressure are completely false.”¹⁸⁷

A Moscow court in early June 2000 agreed with Media-MOST that the police raid was illegitimate. The court ordered the return of the documents seized by the police. The Prosecutor-General’s Office stated that it would appeal the court’s decision.¹⁸⁸ Media-MOST also filed suit against the FSB.

A district court in Moscow ruled in favor of Media-MOST in its lawsuit against the FSB for “slandering its business reputation” as a result of information the FSB made public in early 2000. The FSB had suggested that Media-MOST was involved in illegal surveillance activities and the distribution of compromising materials. The court held that the FSB must apologize for its indiscretion on ORT television during prime time. But Aleksandr Zdanovich, head of the FSB’s public relations center, said that the court lacked jurisdiction and that the FSB would not follow its orders.¹⁸⁹

The FSB sued Media-MOST—obviously seeking revenge—and its newspaper, *Segodnya*, because of articles suggesting that the FSB put pressure on the justice system concerning holdings of owner Gusinsky. The FSB suit claimed that “*Segodnya*” was “undermining the professional reputation” of the FSB and demanded that “*Segodnya*” acknowledge that its reporting was “false.” In December 2000, a Moscow court agreed with the FSB and ordered

Media-MOST holdings and its “*Segodnya*” newspaper to publish retractions of their statements.

In addition, Russian security services became increasingly sensitive that the United States might be using public information to develop intelligence about Russia. The FSB wanted to restrict the public flow of such information. According to previous press reports, American intelligence agencies have noted the potential significance of open sources.¹⁹⁰

In September 2000, Russian political figures sharply criticized the classification of portions of the state budget concerning the government’s media activities. This classified section includes rubrics, such as “information countering” and outline expenditures of 200 million rubles (\$7 million).¹⁹¹ These budgetary arrangements reflect decisions codified in the National Information Security Concept that Putin approved in June. This document, drafted by former KGB officers, identified both external and internal media enemies and thus recalls the work of the Soviet-era KGB Fifth Directorate, which worked against “ideological diversions.”¹⁹²

The National Information Security Concept has also led to a crackdown against journalists and the media. In November 2000, then Russian Security Council Secretary Ivanov said that the new information security doctrine not only imposes constraints on dissemination of secret information but also on the use of unclassified information “obtained in an illegal way.”¹⁹³ This was clearly shown between 10 and 17 November 2000 when FSB and military procuracy officers searched investigative journal *Versiya*’s offices during an FSB investigation on the “Kursk” disaster. The FSB was particularly interested as to the source of a published satellite photography purportedly showing a damaged US submarine in Bergen after the sinking of the “Kursk” in the Barents Sea. The photograph could have been leaked to the media by the military, which maintained that the “Kursk” sank as a result of a collision.¹⁹⁴ The photos, according to the Glasnost Foundation, served as the basis for a criminal investigation.

Norwegian experts, however, said that the photo was a fax and included a Norwegian vessel, which sank four years previously. Photos later published by *Versiya* are spy satellite photos of British and Norwegian navy bases.

On 10 November, the FSB confiscated the desktop computer of Dmitri Filimonov—*Versiya*'s investigation desk editor. Filimonov was also interrogated for four hours about who gave him the photo; the FSB later removed the editor's documents relating to the "Kursk." According to Filimonov, he had received the photo from an "unknown person who gave him a diskette with information in an envelope."¹⁹⁵

On 25 April 2001, Andrei Luchenko, Military Procuracy spokesman, said that officers of his agency searched the apartment of Valeriy Shiraev, the deputy chief editor of *Novaya Gazeta*.¹⁹⁶ Luchenko said that the search was not because of Shiraev's journalistic activity but because he is a former FSB employee. He said that military prosecutors have opened a criminal case against him and several other Media-MOST security officers who have intelligence backgrounds for "divulging state secrets."

The Roots of Putin's Attack on Media Freedom¹⁹⁷

Russian President Vladimir Putin's current campaign against independent media outlets has its roots in Russia's National Security Information Doctrine (NSID), which was drafted by the Presidential Security Council and approved by Vladimir Putin at the end of June (2000), represents a serious challenge to the still-fragile independent mass media of the Russian Federation. Despite its breadth—this 40-page document covers everything from the development of the national telecommunications market to questions of intellectual property—the new doctrine is united by a single idea: the need to increase governmental control over the flow of information by establishing a legal basis for such control.

The NSID was prepared by people whose careers dispose them to conceal and manipulate information rather than to make it public. More than 90 percent of the staff of the Russian Security Council consists of former KGB generals. In preparing this document, they co-opted the seven administrators of the newly created superdistricts, five of whom have military and intelligence agency backgrounds.

While nominally committed to freedom of the press and the prohibition of censorship, the document includes language, which appears to subvert these general principles. According to the newly approved doctrine, individual Russian citizens currently face a number of threats from the media, including the "use of the mass media for restriction of the human right for the freedom of conviction," "the propaganda of mass culture based on a cult of violence and values in violation of norms accepted by Russian society," and "the misuse of freedom of information" by the media.

Russians, the document continues, face even greater threats from abroad, including "the activity of foreign states, international terrorist and other criminal entities, organizations, and groups directed at infringement of the interests of the Russian Federation in the information sphere, reduction of state influence on the life of society, and diminishing economic ability of the state to protect the lawful interests of citizens, society, and state in the informational sphere," and even "growing dependence of the spiritual, political, and economic life of the country on foreign information structures."

Such sweeping statements perhaps portend a darker future for media freedom in Russia, but the doctrine's first fruits have begun to appear already. On 22 June, for example, Putin signed an amendment to the press law that bans "the dissemination and propaganda" in the mass media and computer networks about "methods and techniques of preparation, production, acquisition, and use" of illegal drugs and their precursors. While many may welcome this effort to fight the scourge of drugs, they may be less pleased by the precedent it sets to fight the freedom of the Russian media.

FSB Legalizes Monitoring of Internet¹⁹⁸

A Russian Communications Ministry directive issued on 25 July (2000)—demanding that all state and private operators of telephone, cellular, and paging communications, as well as Internet service providers, open their lines to monitoring by the Federal Security Service (FSB)—has sparked remarkably little controversy in Russia.

According to the directive, the operators of wiring and nonwiring communication companies must design and install monitoring and eavesdropping equipment configured for their networks. These firms must also obtain FSB approval of the system, known by its Russian abbreviation of SORM. Further, the operators must reveal to the agency all access keys to their networks, and the operators must integrate the SORM into their networks, get certification of the equipment from the agency, and train the FSB officers working with the equipment.

The document places particular stress on the principle that all information on SORM must be kept secret, and the FSB should use SORM without the knowledge of the network clients.

When the SORM project first surfaced in 1998, it caused a public uproar in Russia. But now, as it has been put into practice, its provisions have sparked little or no controversy. On 22 and 23 August, “Segodnya” explained this lack of reaction by the division between providers and users. Most Russian telecommunication providers are inclined to accept SORM regulations as regrettable but inevitable. Some even argue that the new regulation does little more than codify existing practice. They claim that the new edict can bring together numerous legal norms or loopholes that give the secret services access to public telecommunications. The only objection these providers have is that they must bear the cost of installing the expensive monitoring equipment.

Users, on the other hand, view this directive as a violation of the country’s constitution. Many of them argue that it points the way to further restrictions on freedom of information and the

mass media. But their voices have not yet found a spokesman in the central media or political system.

In October 2000, Sergei Kabanov, an FSB officer, argued in an article posted on <http://www.fsb.ru> that government monitoring of communications under the SORM system would be undertaken exclusively as part of the fight against crime and espionage. He asserted that the FSB has stayed within the law and became a member of the Russian Association of Document Telecommunications. But he failed to mention that almost half of the crimes against which SORM nominally is directed are not under FSB’s tasks.

Crackdown on Russian Scientists

A special problem for the FSB is the control of Russian scientists, many of whom possess or have access to valuable defense and R&D information. Like their US colleagues, many Russian scientists believe that free access to information and ideas is vital to progress in their field. They chafe at security restrictions and do not always respect them.

Many of these Russian scientists feel the need to remain informed on developments outside Russia in their areas of expertise and seek contact with Western counterparts. This is of special concern to the FSB because of fears that Russian scientists are attractive recruitment targets by Western scientists working for CIA or other foreign intelligence services. In an attempt to control and possibly discourage any long-term or social contact with foreign scientists, new restrictions have been promulgated.

In addition, Russian intelligence services have used a list of state secrets, falling under more than 700 rubrics, that was prepared by the Defense Ministry even though the presidential-approved list includes only 22 secrets.¹⁹⁹ Because of that confusion, there is a lack of clarity in Russian regulations about what is a secret and what is not, which is increasingly a problem for the courts. Over the last several years, the FSB has reported arresting 13 spies as well as preventing “35 attempts to

transfer classified information abroad”—including Nikitin and Grigoriy Pasko, who were charged with disclosing ecological information abroad; diplomat Valentin Moiseyev, who was sentenced for giving the draft of a treaty to South Korea; and Aleksandr Sakov, who was accused of giving job-related information to an Israeli encyclopedia.

Gennadiy Mesyats, the deputy president of the Russian Academy of Sciences, acknowledged that the Russian authorities have imposed new restrictions on scholars’ foreign contacts, but he said that the state is “entitled to hold its scientists to account” and that “the whole business has been blown out of all proportion.”²⁰⁰ One newspaper article reported that the rules represent “a throwback to the Soviet era” and will become obstacles to research.²⁰¹ Meanwhile, it was reported that voluntary informers reporting to the Interior Ministry, the FSB, and other security agencies now number in the thousands.²⁰²

Russian scientists said that they would largely ignore the directive. One scientist said he had seen the directive but “did not pay much attention to it.”²⁰³

FSB Takes Charge of Chechen Operations

By a decree, in January 2001, President Putin presented FSB Deputy Director German Ugryumov with the Hero of Russia order for his work in Chechnya. An admiral, Ugryumov supervised the FSB Department for the Protection of Constitutional Order and the Struggle Against Terrorism, as well as being in charge of the Alfa and Vypmel Special Forces units.²⁰⁴

Later that same month, Putin placed the FSB in charge of the Chechen campaign. Declaring that the Chechen operation had entered a new and final phase, Putin transferred control of military actions there from the Defense Ministry to the FSB, Russian and Western agencies reported. FSB Director Patrushev was to have overall control with Ugryumov having day-to-day responsibility. Security Council Secretary Ivanov said that Putin’s decision was logical because basic combat operations were completed; though

opinion polls show that more than half of all Russians do not believe that there has been any change there in the last year.

Gennadiy Solovev, FSB first deputy director of the department for the defense of constitutional order and combating terrorism, told Duma deputies investigating missing persons in Chechnya that Moscow should restore the practice of passing sentence on accused criminals in absentia.²⁰⁵

Celebrating Chekist Day Again

After the fall of the Soviet Union in 1991, celebration of Chekist Day became almost non-existent. Only a few people marked the day, but no officials from the government did so. Putin, who was then serving as Prime Minister, revived the celebration.

Speaking at a Kremlin celebration of the “Day of the Security Services Worker,” President Putin noted that in the past, “Chekists²⁰⁶ have been blamed for the mistakes and crime of those who were at power.” But now, he said, the secret agencies are serving “not individuals but the country as a whole.” That same day, practically all-Russian media featured stories about and interviews with present and past Chekist leaders. FSB chief Patrushev said that former KGB cadres entering other government agencies reflected the need to introduce “fresh blood” into the political system. Former SVR chief Sergei Lebedev stated that, in the course of the 20th century, “there has not been any place on the planet where a KGB officer has not been.”²⁰⁷

The SVR celebrated not only the anniversary of the Cheka but also the anniversary of the establishment of its immediate predecessor—the foreign department of the OGPU, which was founded in 1920. Putin went to SVR headquarters for the celebrations. Others taking part in the commemoration were former KGB/SVR chiefs—Kryuchkov, Shebarshin, Primakov, and Trubnikov—as well as some of its most famous agents and spies, including British defector George Blake.

In addition, the SVR marked its 80-anniversary by opening its own Internet site at www.svr.gov.ru. The site reports briefly on its current activities and more extensively about the past glories of the KGB, including special pages on Pavel Sudoplatov and the activities of Kim Philby and the Cambridge Five.

Public Perception of the FSB

According to a monitoring.ru poll in early 2001, 42 percent of Russians had a positive view of the FSB, with only 19 percent of the 1,600 people polled having a negative one. The poll also found that 39 percent supported the consolidation of all Russian intelligence and security agencies into a single body like the KGB; 22 percent said they opposed such an approach.²⁰⁸

In June 2001 nearly 60 percent of Russians said they have confidence in the FSB, up from 44 percent in 1995. Sergei Grigoryants, the head of Moscow's Glasnost Foundation, said "members of the security services are not only proud of themselves, they are also sure that they have come to power in the past couple of years."²⁰⁹

Putin: A Reflection of Andropov

In looking at Putin's past, the American press continuously noted his KGB background—serving in the KGB for 17 years and then chief of the FSB before his prime minister appointment. He has spoken fondly of his KGB work and compares himself to Yuri Andropov, a former KGB chief and later head of the Soviet Union for a short period in the 1980s.

Like Andropov, Putin has tried to create the impression that he himself holds liberal views and has succeeded thus far in convincing some foreign observers of this. He is far from being a liberal. His regime is trying to assert more authoritarian political control over Russia. Putin determines government policy for the FSB.

Likewise, Andropov is hardly a model for anyone embracing democratic principles. Andropov favored "repression at home and abroad, spearheading vicious campaigns against dissidents, nonconformists and many others during his tenure at the KGB." Putin is doing the same thing.

When asked about the FSB's repressive policy against Russia's environmentalists, Putin denigrated their motives and attacked their character. He also blamed their existence and machinations on the Western press, foreign diplomats, and foreign intelligence services.

His and the FSB's regressive policies against some Russian citizens have not raised much concern from the Russian public. The political standing of Putin, like the FSB, has risen appreciably.

If Putin does push back the clock and resurrects the old KGB, it will be bad news for the United States and for the Russian democratic process.

Specific Cases

The FSB continue to be suspicious of foreigners and to closely monitor their activities in Russia. The aggressive and hostile attitude by the FSB derives from a mindset inherited from the Tsarist intelligence service called the Okhrana. For example, an FSB spokesman said on 5 September 2001 that FSB officers have broken up an espionage operation by an unnamed South Asian country and have secured the expulsion of the foreign nationals involved.

The former head of the FSB's legal department, Lt. Gen. Sergei Diakov, said that his former agency had acted correctly when it charged journalist Pashko, scientist Igor Sutyagin, and others of "divulging state secrets," even if the information they had in hand was classified or even had been published.²¹⁰ According to Diakov, publication of unclassified information could be a crime if compromises state secrets. Diakov further added that revealing state secrets through negligence

or preparing to disclose state secrets are actions falling under the terms of espionage statutes. And any journalist who obtains information that turns out to be secret can be charged as well.

The FSB sees American travelers as the main threat to the internal security of Russia. It certainly would be to their advantage to nab such a traveler performing an act of espionage or be in a compromising situation, which the FSB could exploit.

Not able to catch “real” American spies, the FSB has turned to “creative” spy cases against Americans either doing business in Moscow or studying/teaching in Russia. The Edmond Pope, John Tobin and Elizabeth Sweet cases are excellent examples of the FSB fabricating false espionage charges against Americans.

The singling out of domestic critics, ecologists and selected groups also points to a resurgence of counterintelligence within the country. Russia has gone through several spy scandals, expelling alleged foreign spies and arresting Russian citizens it accused of espionage. Although several of these cases proved embarrassing, senior government officials have increased their political support for the FSB. In addition, the press articles highlighting the need for a strong FSB suggest that the FSB will continue to take a hard line against Western commercial or academic research in Russia.

Former GRU officer, Col. Stanislav Lunev, probably summed it up best when he said that, “if it can happen to an American citizen, it would be hard to expect any justice and fair treatment for ordinary Russians, who have practically no legal rights and are totally dependent on the special services. Increased powers for these services mean nothing else but a new repression against Russians and more newly fabricated so-called spy cases against Americans and other foreigners rash enough to do business with Russia and uncooperative with its special services.”²¹¹

Lt. Col. Sergei Avramenko

On 10 July 2000, a Moscow court sentenced Lt. Col. Sergei Avramenko, a Russian military officer assigned to a Defense Ministry’s scientific research institute, to four years hard labor in a maximum-security penal colony for photographing top-secret documents detailing developments in Russian military aircraft electronics. The FSB said Avramenko had worked at the research facility for 15 years and decided to photograph the documents before retiring. He tried to take the documents to an unidentified foreign country in May 1996 and sell them but was foiled by a counterintelligence operation. FSB Promotion Programs Department Chief Aleksandr Zdanovich said that, by its actions, his agency had limited the damage Avramenko might have inflicted on Russian national interests.

Anatoly Babkin

The FSB launched a new round of interrogation of Professor Anatoly Babkin of the Bauman Higher Technical University, who was accused of espionage in 2000 together with US Navy engineer Pope. Earlier questioning was suspended after Babkin suffered a heart attack, but FSB officials insisted that Babkin’s health has sufficiently improved to allow him to face investigators. It was speculated that the renewal of the case might in fact be in retaliation to the arrest of Robert Hanssen (see separate entry on Hanssen) in the United States.²¹²

Valentin Danilov

The Krasnoyarsk branch of the FSB indicted physicist Valentin Danilov on charges of spying for China. Danilov, a researcher at Krasnoyarsk Technical University in Siberia, was arrested on 16 February 2001. He faced charges of high treason for passing state secrets to China. The charges are based on a contract between the university and a Chinese company to study the influence of space radiation on satellites.

Danilov was arrested for passing information that the authorities say was classified, but Danilov and his colleagues argue that it was open source. A group of his colleagues published an open letter saying that recent FSB actions mean that in Russia today “any physicist can be a spy,” regardless of what he does.

On 29 April 2001, FSB officials in Krasnoyarsk brought an additional charge of fraud against Danilov.

On 18 June 2001, Danilov charged that the FSB was using psychological pressures to try to force him to confess to a crime he did not commit. The next day he suffered a heart attack and was hospitalized. Danilov remained handcuffed to his bed and under the surveillance of two guards.²¹³

Twenty colleagues of Danilov sent a letter to the Krasnoyarsk Krai prosecutor saying that the lack of substance to this charge shows that, from now on, any physicist can be charged with being a spy.²¹⁴ Russia authorities announced that Danilov would be tried in a closed courtroom.²¹⁵

Danilov’s lawyer announced in August that he finished studying the case materials, which paved the way for the trial to begin.

Lt. Col. Andrey Dudin

FAPSI Lt. Col. Andrey Dudin initiated contacts with the German intelligence agency BND—Bundesnachrichtendienst. The FSB investigation proved his guilt beyond question, and in April 1997, Dudin was sentenced to 12 years.

Major Dudinka

The arrest of an RVSN [Strategic Missile Forces] officer was reported in March 1997. Major Dudinka was trying to sell information to a foreign intelligence service for \$500,000. He had put highly sensitive information on a diskette concerning the command and control system for a missile army and troop location information. According to FSB Director Kovalev, if he had succeeded, the RVSN would not have any secrets left.

Maj. Igor Dudnik

In December 1995, FSB personnel detained Maj. Igor Dudnik, a retired officer of the Russian Center for Space Reconnaissance, at a Moscow metro station as he was handing over top secret satellite photographs to Israeli intelligence operative Reuven Dinel. Further investigation by the FSB determined that Dudnik was not acting alone, but with two accomplices, one of whom continued to serve in the Center for Space Reconnaissance of the GRU. All three were arrested. Dinel, working in Moscow under cover as an Israeli Embassy secretary, was declared persona non grata and expelled from Russia.

On 23 March 1998, Dudnik was sentenced to 12 years in prison for selling classified data to the United States.

Moisey Finkel

Finkel was convicted of espionage after passing information on secret defense research to CIA representatives for monetary reward. According to Russian media, CIA recruited Finkel, a Navy scientific research institute employee, to provide information about new-generation Russian nuclear submarines.²¹⁶ Finkel was a specialist in hydroacoustics. The FSB said he agreed to cooperate not for money but to get political refugee status for his wife and mother-in-law.²¹⁷

Makarov

At the end of June 1997 the Moscow City Court sentenced a certain Makarov, an adviser in the Commonwealth of Independent States and Baltic Division of the Consular Services Department of the Ministry of Foreign Affairs, to seven years imprisonment. The FSB established that the CIA recruited Makarov in the spring of 1976, when he was working at the Soviet Embassy in Bolivia. He continued his espionage activity during official assignments abroad. He was stationed in Spain from 1989 through 1991. Makarov provided a large quantity of secret information to the CIA and received \$21,000 for his services.

Valentin Moiseyev

The FSB arrested Foreign Ministry official Valentin Moiseyev on 4 July 1998 while Moiseyev was meeting with a South Korean diplomat in his apartment. The FSB also arrested the South Korean diplomat Cho Sung-woo and detained him for a while despite his diplomatic status. Russia later expelled the South Korean diplomat.

Moiseyev was accused of spying for South Korea. The FSB said that the South Koreans recruited Moiseyev while he was serving at the Russian Embassy in Seoul in 1992. After his return to Moscow in 1993, he began to pass Russian state secrets to South Korea while meeting with one of its diplomats. During that time, Moiseyev was head of the Korean Department in the Foreign Ministry.

He was tried and convicted by a Moscow City court in December 1999. However, on 27 July 2000, the Russian Supreme Court voided the sentence. The Supreme Court held that his conviction was obtained with evidence that had been illegally acquired. But at the same time, it handed the FSB a small victory in ordering Moiseyev to remain in custody while telling the FSB that it should look for additional evidence.

On 24 July 2001, Moiseyev demanded that the Russian Supreme Court hear his case. Moiseyev's lawyers said he did so because his trial has been shifted four times to different judges and each time the trial has had to begin again. However, his request was denied and the Moscow City Court conducted a second trial.

On 14 August 2001, the court found him guilty and sentenced him to four and a half years but said that his previous confinement in jail would count toward the prison time. The court also said that all property of Moiseyev should be confiscated.

His lawyer said that another appeal to the Russian Supreme Court would be made but noted that by the time it took to process an appeal Moiseyev's prison term would probably be over. The lawyer also accused the court of divulging Russian State secrets, noting that the court revealed that Moiseyev was a former KGB agent.

Alexandr Nikitin

Alexandr Konstantinovich Nikitin, born 16 May 1952 at Akhtyrka, Sumskaya oblast in the Ukraine, graduated from the Sevastopol Naval Engineer College. He served in the Russian Northern Fleet until 1985. Between September 1985 and July 1987 he studied at the Kuznetsov Naval Academy in Leningrad. After graduating from the Academy, he served in Moscow at the Inspection of Nuclear Safety of nuclear installations of the Russian Defense Ministry.

In 1996 the FSB arrested Nikitin and charged him with espionage and damaging the security of the Russian Federation. He was accused of collecting state secrets with the aim of passing the data to a foreign organization. Nikitin reportedly obtained the classified information from his job as an inspector of nuclear installations, which included the Northern and Pacific fleet nuclear submarine bases, the bases of nuclear submarines on special assignments and laid-up ships, all shipyards and ship-repairing enterprises. The charges also stated that, in September 1995, Nikitin passed this information to a representative of a foreign organization in Murmansk.

In November 1992, because of staff redundancies and his own desire, he retired as a captain and moved to St. Petersburg with his wife. When he retired he signed a secrecy agreement not to disclose information pertaining to state secrets to which he had access or learned during his naval service.

On 12 January 1994, Nikitin obtained a passport. In February and December 1994 and April 1995, he used this passport to travel to Norway. While in Norway in February 1994, he met Robert Bathurst. The FSB stated Bathurst, an employee of the Norwegian Institute of World Problems (PRIO), had previously served in US intelligence.

According to the FSB investigation, Nikitin and Bathurst corresponded with each other, and in the spring of 1994, in Murmansk, Bathurst introduced Nikitin to representatives of the Norwegian public organization "Bellona." They asked him to review

Version No. 1 of the organization's report, "Sources of Radioactive Pollution in Murmansk and Arkhangelsk Areas."

After reading the report, Nikitin wrote a review and sent it to Bellona in Murmansk. Nikitin also maintained contact with their representatives by phone and during trips to Murmansk. In the winter of 1995, Nikitin signed an independent contract with Bellona for a fee of US \$1,200.

The contract called for Nikitin to write sections of Version No. 2 of the Bellona report, later titled "The Northern Fleet—Potential Risk of Radioactive Pollution of the Region," using his knowledge and to act as a consultant to Bellona.

From February to September 1995, Nikitin wrote the text assigned to him. The FSB stated that, in August 1995, Nikitin asked his acquaintance, V. L. Rudenko—a retired Navy officer also from the Inspection of Nuclear Safety of Atomic Installations in the Defense Ministry—about special literature on accidents aboard nuclear submarines. Nikitin was told that such literature was available at the first Central Scientific Institute of the Armed Forces of the Russian Federation, at the Main Technical Management of operation and repair of the Russian Navy, and at the Naval Academy.

In order to get access to this literature, Nikitin called V. S. Artemenkov—an acquaintance and senior lecturer at the Naval Academy—on 7 August 1995. He asked for permission to enter the Navy's special library containing literature on nuclear accidents onboard nuclear submarines.

Knowing that Nikitin was a retired Navy officer with access to Secret and Top Secret information, including the data on nuclear reactors on the nuclear submarine fleet and surface ships, Artemenkov told him that such literature indeed existed in the Academy's special library. He agreed to provide Nikitin with this literature and arranged for Nikitin to visit the Academy the next day.

On 8 August 1995, Nikitin used his officer's identification card and the pass signed by Artemenkov to enter the Naval Academy. He reviewed the Top Secret books "Incidents Onboard Nuclear-Powered Submarines 1965-1983," issued in 1987, and "Technical Malfunctions Onboard Nuclear-Powered Submarines of the Navy 1984-1987," issued in 1990. He also reviewed the secret books "The Description of the Common Incidents Onboard Vessels and Service Boats of the Navy in 1989," issued in 1990, and "Description of the Common Incidents Onboard Vessels and Service Boats of the Navy in 1991," issued in 1992.

The FSB said Nikitin copied specific information about accidents and incidents on Soviet nuclear submarines from 1965 to 1989. Specifically, the FSB cited six examples from the Top Secret book "Incidents Onboard Nuclear-Powered Submarines 1965-1983" (1987 edition) and two examples from the Top Secret book "Technical Malfunctions Onboard Nuclear-Powered Submarines of the Navy 1984-1987" (1990 edition).

- Pages 103-104—information concerning an accident that occurred when the reactor parameters were checked while the Soviet nuclear submarine K-27 was at full speed. According to the FSB, the expert commission at the General Staff of the Russian armed forces concluded on 10 June 1999 that the information disclosed failures and peculiarities regarding the construction and operation of nuclear submarine K-27 as armament and military technology.
- Pages 95-96—information concerning an accident on the nuclear submarine K-140 that occurred while modernizing work were carried out. The expert commission ruled that the information about K-140 disclosed information on construction failures and peculiarities regarding the durability of domestic nuclear reactors installed at nuclear submarines and also about the usage and operation of nuclear submarines as armament and military technology.

-
- Pages 104-106—information on an accident aboard the nuclear submarine K-123 as a result of a steam generator operation and emission of coolant into the reactor-compartment. The expert commission concluded that this information disclosed secrets about construction failures in the nuclear power installations, about the nuclear submarine as military technology, and about the usage of newly developed nuclear power installations in military shipbuilding.
 - Pages 97-99—information about an accident on the nuclear submarine K-222, which occurred while the submarine was being repaired at a naval shipyard. The expert commission concluded that the information about K-222 disclosed construction failures and peculiarities in the automatic control system of domestic nuclear reactors installed on nuclear submarines and about the usage and operation of the control system of armament and military technology.
 - Pages 96-97—information about an accident on the nuclear submarine K-320, which occurred while the submarine was under construction and hydrologic tests were carried out. The expert commission ruled that the information disclosed construction failures and peculiarities in the construction and operation of the nuclear submarine as armament and military technology.
 - Pages 67-71—information about an accident on the nuclear submarine K-192, which occurred when the submarine was returning from active service to its base. The expert commission said that the information disclosed peculiarities in the construction of the nuclear reactors and failures in the operation of domestic nuclear reactors installed on nuclear submarines.
 - Pages 53-54—information from the publication “Technical Malfunctions” about an accident on the nuclear submarine TK-208 that occurred during an ordinary start of the nuclear installation. The expert commission said the information disclosed data about failures and peculiarities in the construction and the operation of domestic nuclear reactors installed on nuclear submarines and about the usage and operation of the submarine as armament and military technology.
 - Pages 54-56—information about accidents on nuclear submarines K-279, K-447, K-508, K-209, K-210, K-216, K-316, K-208, K-462, K-38, K-370, K-371, K-306 and K-367 and concerning the bodies of indemnification, regulation and emergency protection, and cases of decompression and leaky steam generators. The expert commission ruled that the information about the above-mentioned nuclear submarines disclosed data about failures and peculiarities in the construction and the operation of domestic nuclear reactors installed on nuclear submarines and also about the usage and operation of the submarines as armament and military technology.
- Each of these revelations violated Article 5, item 1, paragraphs 2 and 4, of the Russian Federal Law “About State Secrets” dated 21 July 1993, No. 5485-1 (with changes and additions 6 October 1997). This information is confidential and constitutes state secrets.
- The FSB investigation further stated that during 19-23 September 1995, Nikitin used the personal computer in Bellona’s Murmansk office to prepare paragraph 2 of chapter 8, “Nuclear-powered submarine accidents.” The FSB said Nikitin added information he had picked up at the Naval Academy, including secret information, and handed it over to Bellona whose representative subsequently forwarded the finalized report, version 2, to Norway.
- The FSB also cited the contract Nikitin signed with Bellona, which called for him to prepare several chapters of the report for a fee. The FSB said that, in writing these chapters, Nikitin described naval reactors of the 3rd generation and referred to construction peculiarities, which he learned while serving in the Navy. In particular he wrote about problems with the circulation, the system of cooling down and equipment for controlling the state of the reactor on various levels of power, and the system of shutting down the reactor when the submarine overturns.

During the prosecutor's questioning at his trial in 1999, Nikitin stated that he neither had committed state treason nor disclosed information pertaining to state secrets. He admitted writing the chapters of the report; however, he said he did not use any secret or top-secret information about nuclear submarines in his work. He obtained all the information from open sources, or he knew that open or public available information existed about the topic. During this period he was computer illiterate, so Bellona employees transcribed his written notes onto the computer.

Nikitin insisted that his information came from memory or open sources. He did not deny that he was familiar with some of the information from his service in the Northern Fleet. He claimed that he well understood which information was classified and that the chapters he had written had no such information. In addition, he explained that he had no access to any classified information after 1992.

Nikitin did say that, while working on the report, some information might have come from secret documents, to which he had access during his naval service. Nikitin said he visited the Kuznetsov Naval Academy several times, including 8 August, when he met with Artemenkov. He confirmed that some information in the report came from books he received from Artemenkov, but he could not remember the specific information.

Nikitin said that when he met Artemenkov the latter produced two top-secret books about incidents on nuclear submarines from his safe. They looked through these books, trying to find information on the level of radioactive pollution in the course of the accidents. According to Nikitin, Artemenkov was present in the room and came to the table at which he sat and they looked through the books together. Nikitin said he found only a few pieces of information, which he copied in his notebook.

Experts of the General Staff analyzed the open literature that Nikitin provided to them. They concluded that the handwritten notes in the notebook that was confiscated at Nikitin's residence

contained transcripts of the above-mentioned secret and top-secret books, which he had used on 8 August at the Naval Academy.

During the court hearing, these experts confirmed their conclusion and specified that the information contributed by Nikitin to the report from the open sources was about 60 to 70 percent, while the rest could not be obtained from the open sources. The experts added that it was not important for them whether the information obtained by Nikitin about the submarines was available in the open sources or not. They were guided only by the decrees of the Minister of Defense, which show if the Ministry declassified the information or not.

The experts repeatedly investigated the open sources of the information, which were used by the defendant while writing chapters of the report. They came to a conclusion that, by compilation of the information from the open sources used by Nikitin, it is impossible to obtain concrete data on design features of the reactors of the third-generation nuclear power submarines given in the report.

The court, itself, examined the open-source literature to try to determine if the experts' conclusion regarding the third-generation nuclear reactors was indeed classified. This examination showed that the complete, detailed data on design features and parameters and the operating description of the cooling system, which operated independently of the batteries on the third-generation nuclear power submarines, were previously disclosed in the magazine "Morskoy sbornik" (4:1995) and in a book by D. A. Romanov.

The court also believed that the events concerning nuclear submarines K-27 and K-123 were revealed thoroughly and in books written by A. Pavlov and N. Mormul, which were published earlier. They pointed out that much information was given in *Jane's Book 1987-1988*, which the experts refused to examine.

The court especially highlighted the search of Nikitin's apartment. It was during this search on 5 October 1995 that the FSB discovered the notebook

and confiscated it. The notes in the book became the foundation for the FSB charges against Nikitin. In looking at the protocol of the search, the court found that this evidence was obtained in violations of Articles 69 and 70 of the Russian Criminal Procedure Code.

The court noted that FSB investigator Osipenko conducted the search at Nikitin's apartment, but when the criminal case was initiated on 5 October 1995, it was given to FSB investigator Maksimenkov. According to the decision made by the chief of the FSB investigation section on 6 October 1995—when the investigation team was established—Osipenko was not included. On 1 April 1996, Osipenko was included on the investigation team by the chief.

During the same time, it was evident from the case files that nobody entrusted investigator Osipenko with conducting the investigative actions, including the search at Nikitin's apartment; therefore, he did not have the right to do so. In consideration of the above-mentioned information, the court found that this evidence—protocol of the search of 5.10.1995—due to the requirements of Article 69, paragraph 3, of the Russian Criminal Procedure Code, was obtained by violating the law and was thus excluded.

The court also stated that, in accordance with Article 29, paragraph 4, of the Russian Constitution, each person has the right to freely seek, receive, pass on, produce, and disseminate information by any legal method. However, in accordance with the provisions of the Constitution, the list of information pertaining to state secrets is stipulated by the Federal Law, while the possible limitations of rights and freedoms of the man and citizen is stipulated only by the Federal Law—Article 55, paragraph 3, of the Constitution.

The court noted that, at the time of Nikitin actions, no such law existed. The only legal act, which regulated the legal relations in the field of protecting the state secrets, became the decree of the Russian president No. 1203 of 30.11.1995.

The court emphasized that the prosecution's use of secret and retroactive decrees as the basis for the case was "in clear violation of the constitution." It stated that the right to environmental information was protected by the Russian Constitution. The court saw no crimes in Nikitin's actions, and it strongly criticized the procedural violations of the FSB throughout the case, starting with its illegal confiscation of evidence back in October 1995.

Based on their view, the court acquitted Nikitin of the charges against him on 29 December 1999. The court said their verdict could be appealed to the Court Collegium on criminal cases of the Supreme Court of the Russian Federation.

When Nikitin was acquitted, the St. Petersburg prosecutor's office immediately announced that it would appeal, and it kept its word. In his appeal against the Nikitin-acquittal, the prosecutor demanded a third City Court hearing, claiming that the acquittal contradicts the facts. More striking, however, is that he wanted the case to be handled "by another judge." Prosecutor Aleksandr V. Gutsan gave no reasons for his claim that the ruling contradicted the "factual content of the case," but hinted that he might come up with more after having "studied the protocol of the court hearing."

The Bellona legal adviser, Jon Gauslaa, believed it would be impossible for Gutsan to substantiate his claim. Two thirds of the verdict dealt with the facts described in the indictment and the evidence of the case. Thus, the verdict was based on the facts. But more important, it was based on the Constitution and not on the secret and retroactive decrees, which was the sole basis for Gutsan's case.

It is easy to understand why the prosecutor demanded another judge. Sergei Golets turned out to be an independent judge. He did not take the FSB's biased allegations for granted but evaluated the case objectively and based his decision on the law.

Although this was a victory for Nikitin, he remained under city arrest in St. Petersburg.

Hans Peter Nordstrem

Hans Peter Nordstrem, a Swedish military intelligence communications officer, was caught carrying out an operation to contact an agent in St. Petersburg and expelled from Russia.

Platon Obukhov

In April 1996 the FSB arrested former Russian Foreign Ministry staffer and British agent Platon Obukhov, who had been passing political and strategic defense information to MI-6. The FSB characterized the case as the biggest British special service failure since the time of Oleg Penkovskiy.

According to the FSB, British MI-6 recruited him when he was serving at the Russian Embassy in Norway. He was given the codename “Plato.” Obukhov, a second secretary in the North American Department of the Russian Ministry of Foreign Affairs, was educated at the elite Moscow State Institute of International Affairs. He is the son of Alexei Obukhov, a former deputy foreign minister and top arms control negotiator, who played a key role in negotiating the 1987 US-Soviet INF agreement scrapping medium-range nuclear missiles.

Obukhov’s arrest led to the biggest spying scandal between London and Moscow since the end of the Cold War. The diplomatic row led to the expulsion of four British diplomats from Moscow and four Russian diplomats from London.

Obukhov’s family insisted that he was mentally ill from early childhood. His family and his lawyers succeeded in delaying his case for more than four years while they attempted to prove that Obukhov was insane and not responsible for his actions.

In 1997 psychiatrists from the Serbsky Psychological Institute in Moscow said Obukhov was suffering from “reactive psychosis,” a mental disturbance he developed only after his arrest. On the basis of this report, the Russian court found Obukhov mentally incompetent to stand trial and remanded him to a psychiatric clinic for treatment.

After 18 months in analysis, Yevgeniy Krylov, a St. Petersburg-based psychiatrist, certified Obukhov mentally fit and able to stand trial.

According to various media accounts, televised footage from the court session seemed to contradict Krylov’s assessment that Obukhov was psychologically fit to stand trial. A bearded Obukhov, wearing jeans and a jacket, appeared pale and visibly agitated. As he stood in the defendant’s cage he talked to himself, prayed, grimaced, and rubbed his cheek and neck.

In late July 2000, the Russian court found Obukhov guilty of spying for the United Kingdom and sentenced him to 11 years in a high-security prison. All his property was ordered to be confiscated. However, in January 2001, the Russian Supreme Court voided Obukhov’s conviction and sentence.²¹⁸ Obukhov’s family and lawyers said that he is mentally ill and that the case against him was fabricated by the FSB.²¹⁹

Oppfelt

The activities of US citizen Oppfelt [as transliterated], who, having made contact with a Pacific Fleet officer, was collecting information of a covert nature on naval facilities, were cut short and he was expelled from Russia.

Valeriy Oyamyae

In March 2000, the FSB arrested Valeriy Oyamyae and charged him with passing secrets to the British and Estonians, using a contact at the British Embassy in Tallinn. Oyamyae, a former intelligence officer, passed information on FAPSI. FSB Chief Patruska said “he (Oyamyae) had been a senior officer in one of Russia’s special services and he was using his connections with officials in enforcement structures and people in political and business circles to gather information.”²²⁰

On 21 April 2001, a Moscow court convicted Oyamyae of high treason and sentenced him to seven years in jail and confiscated his property.”²²¹

Grigory Pasko

Grigory Pasko, a naval captain and military journalist for the newspaper of the Russian Pacific Fleet *Boyevaya Vakh*, was charged in November 1997 with espionage and revealing state secrets. The FSB classified the case a state secret, making it difficult for his lawyers to mount a proper defense. Pasko's "crime" was reporting on the Russian Navy's illegal dumping of nuclear waste in the Sea of Japan.

Pasko came to the attention of the FSB because of his contacts with Japanese journalists in Vladivostok. The Japanese were in the area because there was some controversy about Russia's disposal of liquid radioactive waste in the territory.

The Japanese had commissioned a radioactive wastewater treatment facility at Bolshoi Kamen. The Japanese Government decided to fund construction of the plant after it was revealed that Russia dumped some 800 tons of radioactive waste from dismantled nuclear-powered submarines into the Sea of Japan.

Funding for the liquid waste storage and processing plant was part of an October 1993 agreement by the Japanese with the Russian Federation to assist in the environmentally safe reduction of its nuclear defense systems, including the dismantling of part of the Russian nuclear submarine fleet. This sophisticated plant, mounted on a 213-by-77-foot barge, is capable of treating 1.8 million gallons per year. The processing system extracts waste contaminants from water used in the submarine decommissioning and dismantling process. The low-level nuclear waste is mixed with concrete, placed in specially designed containers and placed in secure storage pending ultimate geologic disposal. The treated water, which meets most drinking water purification standards, is returned to the sea.

Pasko, in an article he wrote, showed the threat to the environment caused by accidents in the decaying Russian nuclear submarine fleet. Because of a shortage of money and high-level corruption in the Pacific Fleet, the Russian Navy had dumped liquid and solid nuclear waste off the coast of Vladivostok.

In May 1999, the Russian media reported that Russia's SVR concluded that Pasko was a foreign spy. The service reportedly said that the Japanese journalists, Takao Dzyun, Tadashi Okano, Nasu Hiroquki, Akihito Sato, and Yamauchi Toshikiku, were all intelligence officers. If Pasko carried out tasking by these officers and received money from them, he was their agent.²²²

The SVR quickly denied preparing the report. However, SVR spokesperson, Boris Labusov, said "It is not within the competence of the SVR to determine whether anyone is guilty or not guilty of any crime." He did say the SVR received an inquiry and "under articles 70 and 88 of criminal procedural code, (the SVR) has given an objective and complete reply to it, of which it cannot comment due to the secrecy of the information it contains."²²³

Human rights groups began to raise concern about the Pasko case. Human rights activists said Pasko's case was similar to that of Nikitin, who was under investigation in connection with his report on nuclear dumping by Russia's northern fleet. Alexei Simonov of the Defense of Glasnost Fund stated that it seems to be more and more difficult to write about environmental issues in Russia. The human rights group Amnesty International declared him a "prisoner of conscience."

Pasko's lawyer, Yaroslav Gerin, said documents that were confiscated from Pasko's house did not support the FSB case. Gerin told a Moscow news conference "Pasko did not have one bit of secret material either in his home or with him." The defense attorney said Pasko was working on some reports on agriculture and shipbuilding for a Japanese magazine when he was arrested.

A third Pasko defense lawyer, Oleg Kotlerov, said the FSB was guilty of a series of legal violations in their handling of the case. According to Kotlerov, the case is not democratic because the hearing is closed—no press is allowed—and prosecutors are using all their power to silence Pasko's lawyers.

Gerin stated that Pasko's health has seriously deteriorated. He has back pain, skin disease, and he

is under great psychological pressure. He says even murderers are not put into solitary confinement.

Pasko's lawyers continued to tell the media that there was no evidence that Pasko did anything illegal. They argued before the court that if anyone is breaking the law, it is the FSB.

The FSB raided his apartment, confiscating his computer, fax machine, and car. He was denied bail and began an extended prison term without a trial. Pasko was actually held in custody for 14 months, including six months in solitary confinement before he had a court hearing in February 1999.

According to Voice of America, the trial of Pasko began after he was led—shackled with handcuffs—by five policemen up the crumbling and poorly lit stairs of the Vladivostok military court. As Pasko was being led in, he shouted, “It’s a gulag (Soviet camps for political prisoners) trial. Record that and tell everyone.”²²⁴ His lawyer told Voice of America that the FSB was using illegal interrogation methods and sleep deprivation to investigate him.

Pasko was tried in a closed hearing by a military judge and two officers. The military judge later postponed the trial for one week so that Pasko could get new lawyers. One of Pasko's lawyers, Kharen Nirsisyan, was expelled from court after asking a witness if he was employed by the FSB. Pasko's defense team wanted the judge to reinstate Nirsisyan. His lawyers also formally protested because they said the presiding judge, Dmitry Savushkin, was biased, and they wanted him to disqualify himself from the case. Instead, Judge Savushkin postponed the trial until 16 February. The defense lawyers said the judge ruled that Pasko could choose new lawyers and that, until the lawyer issue is resolved, the judge would not address the question of his personal bias. They added that Pasko did request four new lawyers, two of them are high-profile human rights lawyers defending Nikitin, who was also charged with espionage and treason.

Kotlerov told the media that Pasko should at least be released from prison. He should not sit in solitary confinement if there is no proof he

committed a crime. His client has already spent 14 months in what Kotlerov called a tuberculosis-infested prison. The lawyer took another swipe at the FSB, calling their methods the same as those of the old KGB, but now illegal. He said agents are not supposed to interrogate a sleep-deprived person for 10 hours at a time.

A local newspaper, called “Vladivostok,” printed an interview with FSB chief of the Pacific fleet Nikolai Satskov. The newspaper reported Satskov said Pasko was not charged as a journalist but as a Navy officer. The newspaper also quoted him as saying Pasko's ecological reports had nothing to do with the charges against him. The matter was more serious because Pasko handed over top-secret information vital to the security of the Pacific fleet.

The Japanese television network finally responded to the case in February 1999. In a letter, an NHK TV chief wrote that the television network did not buy any “secrets” from Pasko. It said the network hired him simply as a freelance journalist.

After the trial resumed, testimony was heard from graphology and handwriting experts who were appointed by lawyers of the court. These experts found serious violations in a protocol compiled as a result of the search of Pasko's apartment. They concluded that different people other than the witnesses of the official search made the signatures on one of the pages of the protocol. They indicated that the page with the forged signatures also had different ink from that which was used on the other pages of the protocol.

Another one of Pasko's defense lawyers, Anatoly Pyakin, told the court that since the protocol was filled in, it violated procedural law and could not be used as evidence in the case. Under article 50 of the Russian constitution, justice cannot be administered using documents obtained by violating the federal law. Pyakin reminded the court of Article 69, which states that evidence obtained by violating the law is invalid in terms of law and cannot be used to substantiate a charge.²²⁵

A FSB agent denied that any corrections were made in the protocol. The authorities also admitted that none of the facts he had published revealed state secrets or endangered national security.

In July 1999 the Russian Pacific Fleet military court in Vladivostok released Pasko after it found that the prosecution lacked evidence to support the espionage charges against him. The military court further ruled that some of the evidence brought against him by the FSB was, in fact, falsified. The court did find Pasko guilty of “abuse of office” under the Russian Criminal Code and sentenced him to the maximum term of three years’ imprisonment. Under the provisions of a general amnesty, the court relieved Pasko of the obligation to serve the sentence.

In November 2000, the military collegium of the Russian Supreme Court opened the way for a new treason trial for Pasko when it cancelled the lower court’s verdict. This decision, Pasko said, would be like “a death sentence” for him, noting that his trial would be in the same court with the same FSB monitors who initially prosecuted him for publicizing information about the Russian Pacific Fleet’s actions that lead to the contamination of the ocean.²²⁶

On 4 June 2001, the trial was to begin but instead was postponed when prosecutors failed to appear in court to request the postponement. Rather, a printed notice on an inner door of the courthouse announced that the case was postponed until June 20. However, this trial date was later pushed back to 11 July 2001.

At his new closed military trial, witnesses failed to prove Pasko was guilty of the treason charges against him. Pasko’s lawyer, Anatolii Pushkov, said that one of the witnesses, the deputy commander of the Pacific Fleet, Vice Admiral Aleksandr Konev, told the court that he personally gave Pasko permission to visit secret sites and make video films there. Another defense witness, Anatolii Fomin, who worked for the same military newspaper as Pasko, testified that he and Pasko secured FSB permission for all their activities.²²⁷

Edmond Pope

In an interview, FSB Director Patrushev said his agency is focused on protecting Russian scientific and technical research and leading-edge technologies and developments “without which the country’s revival would be impossible. And here the case of Edmund Pope, a former career US Navy officer, is significant.



Edmond Pope arranged to have dinner with Professor Babkin on 3 April 2000 at a Moscow restaurant. Pope had previously contracted with Babkin for information on the Shkval torpedo, which is used in Russian submarines. Pope had received four reports from Babkin, a professor at Moscow’s Bauman University, who, with several university colleagues, had designed the torpedo. Pope paid \$28,000 for the reports. A Pope-established company Tech-Source Marine Group was to receive a fifth report from Medas, a Russian firm. These firms were established to circumvent the US embargo on certain technology transfers.

At the dinner meeting, Pope intended to tell Babkin that he would not be using Babkin. He made this decision when Daniel Kiely, a Penn State research official who acted as Pope’s technical expert, advised Pope that the Shkval information was too general and mostly public knowledge. That evening, the FSB burst into Pope’s hotel room. They detained him, Kiely, and Babkin. The FSB forced Kiely and Babkin to sign confessions that they had trafficked in state secrets. Kiely was then released. Pope was charged with stealing Russian state secrets.

Russian media quoted the FSB as saying that Pope tried to obtain plans to the high-speed Shkval. Pope said he was innocent. He stated that he bought the Shkval design from Babkin and added that the rector of Bauman University also knew about the purchase. After his arrest, Pope was taken to Lefortovo Prison.

Pope is a former US Navy captain who worked in naval intelligence. In 1994, he retired from the Navy after a 25-year career—his last two posts were director of security in the Office of Naval Research and as an intelligence adviser in that office. He then worked for Penn State's Applied Research Lab for three years. In 1997 he formed CERF Technologies International.

Pope also suffered from a rare form of bone cancer, which was in remission. His wife, however, feared that his imprisonment would reactivate his illness and might cause his death. Pope's wife and defense attorney made efforts in getting Pope released from prison until his trial, but their efforts failed. Pope's wife turned to Congressman John Peterson R-PA, who called on the Russian Government to allow Pope to be examined by independent doctors at a Moscow clinic. The Russian court refused, saying that Russian doctors said Pope was fit to stand trial.

President Clinton, Secretary of State Madeleine Albright, and other senior Administration officials pressed the Russian Government to release Pope from prison. The US Department of State sent numerous protests to Russian officials, warning that Pope's continued confinement endangered his health. In response, Russian President Putin said that Russia's court had to decide Pope's fate.

The Lefortovo district court again ruled in August 2000 against any pretrial release of Pope.²²⁸ The Russian authorities also refused to allow an American doctor to examine Pope, who reportedly suffers from cancer. An FSB spokesman said his organization knew about a US State Department protest concerning Russian treatment of Pope. But, he added, "our medical experts find no pathology in Pope's condition."²²⁹

To try to counteract the pressure being applied to release Pope and bolster its own case, the FSB released a statement in August. The FSB said, "The patterns and methods of Pope's work as the director of a private commercial organization matched the pattern of gathering military information for the United States."

In September a Moscow court again refused to release Pope so that he could receive medical treatment. The court said that he was not ill enough to justify his lawyer's request.²³⁰

The Russian procuracy's public information service issued a press release on 27 September, saying that prosecutors had turned over Pope's case to the courts. So far, Moscow has ignored US demands for his release on bail. An unnamed FSB officer stated that the Russian Government was not planning to swap him for convicted Russian spy Aldrich Ames, as some rumors had said. "The damage Ames caused to the US is incomparable with what Pope did to Russia," the officer said. But he did not exclude that, after Pope is convicted, he might be exchanged for George Trofimoff, a retired US officer who spied for the USSR and the Russian Federation.²³¹ Putin also told Larry King on CNN that he would not consider any suggestion to swap Pope for Ames.

The trial began on 18 October 2000. During the trial, Pope's defense lawyer requested that a new interpreter be appointed. The defense lawyer told the court that the current interpreter assigned to Pope was working for the FSB and also adding comments when translating. The court refused the request.

Babkin initially testified against Pope and then recanted his testimony and said the American had done nothing wrong. Babkin also gave Russia's independent NTV television network a tape recording of FSB agents threatening to send him to "Siberian prison camps" unless he stuck to his original confession.

Yeygeny Shakhidzhanov, general director of the Region State Science Company, which manufactures the Shkval, said, "We did not give

him anything secret. The technology is unique, there is nothing like it to date, and it costs a tolerable amount of money.” The State prosecutor, Oleg Plotnikov, acknowledged the Shkval was declassified but said its fuel and other components were still secret.²³²

Professor Arsenii Myandin said that the information Pope was accused of obtaining via espionage was unclassified and placed in the public domain a long time ago. Myandin, who designed the Russian naval missile “Shkval,” said that he had lectured about it and even published all the details concerning this weapon in a book that was declassified in 1991. But Russian prosecutor Oleg Plotnikov said that Myandin’s testimony had failed to convince him.²³³

Georgiy Longvinovich, the chairman of a special “experts commission,” convened to deal with charges against Pope. Longvinovich said that its members “unanimously” believe that the materials Professor Babkin gave to Pope were secret.²³⁴ The FSB stated “Certain technical decisions related to this unique product remain secret and preventing their dissemination permits Russia to keep its superiority in this field even if finished models are sold.”²³⁵

To rebut Longvinovich, Pope’s defense lawyer presented the court with nonclassified technical reports identical to those Pope received from Babkin. Pavel Astakhov said the reports had been compiled exclusively from public periodicals and books published by teachers of the Moscow Aviation Institute.

At the same time, in an illogical remark, a prosecution witness said that statements on Pope’s behalf by President Bill Clinton and Secretary of State Madeleine Albright proved that “Pope is not a simple businessman but rather a career intelligence officer.”

The Pope case generated concern by a group of Russian nuclear and military scientists, which appealed to the Russian Security Council, the FSB, the Justice Ministry, and the Duma to improve the protection of state secrets and impose greater punishments on those who compromise such

secrets. They said that such actions were necessary because of American activities, including pressure on Moscow regarding Pope, an accused spy.²³⁶

On 21 November 2000, Pope’s lawyer, Astakhov, asked the court to throw out all evidence presented by the state prosecutor Plotnikov and to suspend Plotnikov from the case. The Moscow city court refused the defense motion, even though the defense showed that Plotnikov’s son, an FSB officer, was one of the investigators of the case. The latter, however, did remove himself from the case by declaring that he was ill. Another prosecutor, Yuri Volgin, replaced him.²³⁷

During the trial, Pope denied seeking any information that was not on the public record, an assertion supported by numerous witnesses at the trial.

For the first time since a Soviet court found U-2 flier Francis Gary Powers guilty of espionage in 1960, a Moscow judge convicted an American of spying. On 6 December 2000, the Moscow court found Pope guilty of espionage and sentenced him to 20 years in prison. Zdanovich, head of the FSB Programs Promotion Directorate, said he was “satisfied” by the verdict. It proves, he said, that Moscow is “decisive” in protecting “state secrets from any encroachments.”²³⁸

After the verdict, Russian Government-controlled media defended the trial and conviction of Pope, while Russian independent media criticized the verdict and warned that US-Russian relations would suffer. Government media insisted that Pope was guilty and played down any danger to US-Russian relations. On 6 December, Zdanovich stated on RTR TV that more “facts” would be disclosed in a film from the FSB.

Nongovernment media—most notably outlets linked to Kremlin foe Gusinsky—cautioned the verdict would “seriously complicate” relations with the United States and damage business ties.²³⁹ Segodnya declared the case “dealt a mighty blow to Russia’s reputation” for justice and the independence of its courts.²⁴⁰ The frequently anti-Kremlin *Moscow Times* condemned the

“arbitrary conviction and punishment,” claiming it demonstrated the courts’ “weakness and unprofessionalism.”²⁴¹

Following the verdict, Pope’s wife and the US Government appealed to Putin for clemency. Although Russian security agencies demanded Pope be given a severe sentence so they could use him in an exchange for a Russian spy, they expected Putin to follow the official commission’s recommendation to pardon Pope. The security agencies held out hope that even after the pardon a spy swap could still be negotiated—Pope for a Russian agent in the United States or somewhere else.²⁴²

On 9 December, Putin pardoned Pope. He said that the pardon would take effect once Pope’s sentence took effect, which was the following week. On 14 December, Pope was released from prison and flown to Germany where he underwent several days of medical testing at a US military hospital. He arrived back in the United States on 17 December.

FSB director Patrushev said the Pope case shows that “in Russia’s murky waters, foreign businessmen-spies have worked freely, buying technologies created by thousands of people for mere kopeks. With Pope, Russia showed this has ended.”²⁴³

Although some viewed the Pope case as a sign of renewed forcefulness by the FSB under Putin, the security service came under criticism for its handling of the case. According to media reporting, Western intelligence officials learned that several months prior to his arrest, Pope was on a FSB list of about 12 US and European defense experts whom the FSB considered targets for criminal charges because of their activities. The FSB probably considered Pope a logical target because of his background in naval intelligence. In the FSB paranoia about spies, “once an intelligence officer always an intelligence officer.” Others saw the case as an effort by the FSB to cover up past ineffectiveness.

Foreign businessmen have always felt comfortable in muddy water. For kopeks it was possible to acquire know-how that had been created through the labor of

thousands of people. In this case, Russia showed Pope that these times had come to an end. The country’s leadership let it be known to the international community that it protects its national interests with strictness and according to principle.”²⁴⁴

*Craig Rucin*²⁴⁵

Craig Rucin, an American Protestant carrying out religious work on a voluntary basis in the capital of the Republic of Udmurtia, Izhevsk (700 miles east of Moscow), was deported from Russia on 21 July 2001. Rucin explained that on 17 July he was summoned to the local OVIR office (the Russian bureaucratic department that deals with the registration of foreign citizens) where he was informed that he constituted “a danger to the Russian Federation.” According to Rucin, an OVIR official had told him that he was under no obligation to give the reason for his deportation since it was “a matter of national security.”

With a one-year business visa valid until January 2002, Rucin had worked for a local cultural exchange company called Slovo (Word), which teaches courses on computer studies—in both Russian and English—to foreign and local citizens. Slovo—partly founded by a Florida-based Protestant missionary organization called Pioneers—changed its name from “Russian-American Christian Professionals Institute” and dropped the religious aspect of its work when it reregistered in 1998.

Attached to Pioneers on an individual basis, Rucin said that while in Izhevsk he had additionally given free training to local Protestant pastors, which he stressed had taken place “in the evenings and at weekends—in my spare time—which should be within my rights.” The 1997 Russian law on religion is hazy in this area. While Article 20, Part 2, states “religious organizations have the exclusive right to invite foreign citizens for professional purposes,” no conditions for nonprofessional or voluntary religious activity by foreign citizens are specified. According to Article 3, Part 1, such activity would appear to come under the

individual right to disseminate religious convictions guaranteed to foreign citizens legally present in the Russian Federation.

On 21 August 2001, plenipotentiary for religious affairs in Udmurtia, Sergei Ilinsky, was unable to state definitively why Rucin had been expelled, but thought that it might be due to his religious activity. “He came here as a teacher of English with Slovo—and religious work is not in accordance with that. It is a violation of his visa and the charter of that organization.”

Ilinsky evidently deemed Rucin’s religious activity to be professional in status despite its voluntary nature, describing it as “training up personnel for local Protestant churches.” “It was perfectly in order for a missionary to do such work if invited by a local Protestant church,” he said, and stressed that many such churches invited foreigners to preach and distribute literature in Udmurtia “without problems.”

In Ilinsky’s view, a further possible factor in Rucin’s expulsion was that “we don’t have a simple republic here—it contains many military installations and there has always been a high degree of vigilance here.” Rucin also pointed out that Udmurtia was a closed zone until *perestroyk*, due to its military installations, commenting, “they are paranoid about outsiders here.”

Rucin’s predecessor at Slovo and a lieutenant colonel in the US Army, Warren Wagner, worked as a supervisor of weaponry disarmament in the Udmurt town of Votkinsk. On 10 August, Wagner—who is now an assistant to the president of Pioneers—wrote that he had been denied a visa to Russia in January 1999. “The foreign ministry regional office in Izhevsk told Slovo representatives that they would not approve an invitation to me. Since then they have been told that I am under a five-year ban.”

Precisely how Rucin’s activity could constitute a danger to the Russian Federation remains unclear. On 27 August the director of Slovo, Galina Aminova, said that she believes his expulsion to be part of a broader anti-Protestant drive on the part of the Udmurt authorities. “It is because he is foreign and a Christian,” she explained. “I don’t think there would

have been a problem if he’d just been foreign—and we are the kind of Christians who do not sleep.”

Rucin also pointed to allegedly FSB-inspired articles in the Udmurt press, claiming his religious work to be a front for the US Government. “They think my real aim is to change the hearts and minds of Russians so that they become more obedient to the US.”

Vladimir Sintsov

On 29 May 1997 the trial of V. Sintsov, a worker at a defense institute, opened in Moscow. He was charged with treason in the form of espionage and the transfer of Russian defense and technological secrets to British intelligence. The British recruited Sintsov in the early 1990s in London when he was serving there as head of the foreign economic relations directorate of Spetsmashinostroyeniye I Metallurgiya AO—a joint stock company. Russian media reported that the British recruited him based on information that Sintsov had accepted 30 million rubles in bribes between 1991 and 1994—primarily for his aid in selecting go-between firms shipping arms abroad.

Not wanting to be exposed, he agreed to cooperate. There were 20 meetings between the British and Sintsov, which took place either at the Olympic-Pena hotel in Moscow or in Western Europe. He received \$15,000 for information on the amounts of shipments of Russians arms, description of a missile system, and performance of up-to-date Russian weaponry. He used computer diskettes to pass the information to the British, as well as sending photocopies of classified documents to them.

His last meeting with the British occurred in January 1994, when he flew to Singapore to meet with them. On his return to Moscow on 15 January 1994 he was arrested by the FSK.

A FSK search of Sintsov’s apartment and office yielded a miniature camera and diskettes containing top-secret information.²⁴⁶

On 2 July 1997, Sintsov was sentenced to 10 years in prison.

Igor Sutyagin

The FSB arrested Sutyagin in 1999 and accused him of spying for the United States. Sutyagin, who works at the Institute for USA and Canada Studies, remained in jail on charges of treason and espionage. At that time, the FSB also searched the Moscow residence of Princeton Professor Joshua Handler, a colleague of Sutyagin, but the security service did not detain him.

Handler reported to the US Embassy in Moscow that FSB officers interrogated him in his Moscow apartment. According to Handler, his interrogation lasted approximately seven hours. He told Embassy officials that the FSB officials who questioned him presented him with a warrant permitting them to search his apartment. They removed a number of items, including his computer. He received a receipt for his property and was told that it would be returned to him in approximately two weeks.

While the FSB said Sutyagin is an American spy, the service appeared to be trying to figure out which foreign intelligence service actually ran Sutyagin. On the one hand, he met openly with US diplomats in Moscow, and the FSB insists that he passed classified information to them. According to the FSB, his open behavior suggested that the US spy agencies might have adopted “a new tactic.”

On the other hand, according to Sutyagin’s colleague, Pavel Podvig, FSB officials believe that Sutyagin was spying for Canada. Sutyagin, in fact, was hired to conduct research on military-civilian relations by two Canadian universities that had funding from Canada’s Department of National Defense. According to a York University official, Russia is the only country of the dozen “where some officials seem to have found a Canadian study of civil-military relations to be a threat to national security.”²⁴⁷

In September 2000, the FSB completed its investigation of Sutyagin and handed his case to the court.²⁴⁸ In order to bolster their case, the FSB leaked stories to the Russian and Western media in order to put pressure on Sutyagin.²⁴⁹ On 28 February 2001, *The Guardian* in England published

an article saying that two of Sutyagin’s British contacts were in fact American spies. The next day, *Nezavisimaya Gazeta* published a story suggesting that Sutyagin had taken money from Western intelligence for information about the Russian nuclear fleet.

At Sutyagin’s closed trial in Kaluga Oblast, Col. Sergei Koshelev, a witness for the prosecution, said that the Russian Defense Ministry believed Sutyagin damaged Russia’s security “by trading information about its weapons to foreign countries.” In an ambiguous statement, Koshelev stated that, although “the information supplied by the defendant to foreign countries did not contain secrets,” it provided insight into the army’s combat readiness.²⁵⁰

Vadim Semyonov, a senior FSB researcher from its scientific research center, confirmed that two officials from the London consulting firm Alternative Futures, with whom Sutyagin collaborated, were foreign intelligence officers. According to Sutyagin’s lawyer, Semyonov and other FSB “specialists” were trying to find out whether the firm’s officials were foreign intelligence officers. The lawyer argued that when Sutyagin was passing information he might have been unaware that the firm’s officials were intelligence representatives.

FSB investigators have asserted that Sutyagin carried on continuous contact with Alternative Futures, one of whose cofounders, Sean Kidd, and employee Nadya Lock are US career intelligence agents. Investigators also maintain that the firm itself is just “a cover” for one of the intelligence services.²⁵¹

Elizabeth Sweet

Elizabeth Sweet, an American teaching English on contract to Omsk State University, discovered that just doing your job can be just as dangerous as being engaged in illegal activities. The FSB in that region accused Sweet of espionage and ordered her to leave the country.²⁵² FSB officials said that Sweet organized her students into a group to collect information about the Russian defense industry.

Sweet's apparent crime was asking her students to prepare a report on the economic state of local enterprises. The FSB looked at the assignment—given by an American professor, as well as her students' zeal—as possible tasking to collect classified information. According to Ekho Moskv radio, "counterintelligence had no grounds to charge the American professor with espionage, so they just expelled her from Russia to be on the safe side." The FSB said that three-quarters of the enterprises on Sweet's list belonged to the defense sector.²⁵³

An FSB spokesman quickly refuted the expulsion order, saying that the mass media "distorted" information about expelling Sweet. He said that the data Sweet collected was not for espionage but to "create a negative image of local industry." He added that rather than expel her from Russia, the FSB "strongly recommended to the local university not to extend her contract."²⁵⁴

John Tobin

John Tobin, a 24-year-old American studying political science at Voronezh State University on a Fulbright scholarship was arrested on 27 February 2001 and charged with possession and distribution of marijuana. The Tobin case gained international attention when FSB officials accused him of being a spy in training. In a case of mirror imaging, the FSB said he had come to Russia to study the language and culture before beginning work for an American intelligence agency—like KGB officers who studied in the United States before embarking on their intelligence careers. However, he was never charged with espionage.

Tobin said he was not guilty of the drug charges and maintained that the marijuana was planted on him because he had refused an FSB recruitment pitch to spy against America. His arrest raised suspicions because it came at a time when the United States and Russia were each accusing the other of spying. Washington expelled 50 Russian diplomats and the Kremlin followed suit, sending 50 American diplomats home.

A Voronezh court on 27 April found John Tobin guilty of marijuana possession and sentenced him to three years in a penal colony. Less than 2 months later—7 June—the same court reduced the sentence. Tobin would now serve 12 months in prison rather than 37 months. Tobin's lawyers said that they would appeal and seek the complete vindication of their client who continued to insist he is innocent of all charges.²⁵⁵

Embarrassed by their having to drop the espionage charges from the prosecution of Tobin, the FSB continued to pursue possible spy charges against Tobin. One of the FSB investigators said his agency believes that the Fulbright exchange program may be serving as a cover for American espionage activities in Russia more generally and must be investigated.²⁵⁶

Meanwhile, Pavel Bolshunov, an FSB spokesman, went further and said that a Russian biologist who was briefly imprisoned in the United States has told the FSB that Tobin presented himself at that time as an FBI agent and tried to recruit the biologist to spy for the United States. But Tobin's lawyer replied that such claims are untrue and are part of an FSB effort to prevent Moscow from releasing Tobin before the end of his sentence.

The FBI said on 27 June 2001 that Tobin was never an agent of the bureau. The Connecticut Department of Corrections, where Tobin was said to have met with the imprisoned Russian scientist in 1997-98, said that Tobin had never been there, adding that a certain Dmitrii Kuznetsov had been incarcerated there at that time for a larceny conviction.

A Russian Justice Ministry spokesman said on 26 July that, if the courts agree, Tobin might be released in early August after serving half of his sentence. The spokesman said that the grounds for such a release might be Tobin's "good behavior" behind bars.

On 2 August, Tobin was recommended for parole. He was freed the next day. He remained in Moscow to await an exit visa, which was subsequently granted. He departed Russia on 8 August 2001.

Others

In July 2000, the FSB detained a 26-year-old Lithuanian citizen on charges of spying for the CIA against the FSB. FSB spokesman Zdanovich said that the ethnic Russian was approached in 1999 and asked to use his computer skills to penetrate the Russian spy agency. Lithuanian officials denied the story, pointing out that the man the Russians say they arrested was in Vilnius. One Russian media outlet suggested that the Lithuanian's detention represented an FSB attempt to retaliate for the arrest in June of retired US Col. George Trofimoff, who was charged with spying for the KGB during the Cold War. Retired KGB officer Sergei Sokolov said Oleg Kalugin, who earlier broke with the KGB and currently lives in the United States, betrayed Trofimoff.²⁵⁷

Targeting Humanitarian Groups

Lt. Gen. Vladimir Bezuglii, the head of the Federal Security Service (FSB) department for North Ossetia, stated that some employees of international humanitarian organizations working in the northern Caucasus are spies. He said that five such people were deported in 2000, and he said "in Georgia, there are several international organizations that are 'covered' by the CIA. Through them, Chechen rebels get food and medicines," he added.²⁵⁸

The FSB in Voronezh said that it began an investigation of a Chechen who previously resided in France. According to the FSB, the unidentified Chechen has confessed to working for French intelligence against Russia. The FSB said that he had collected information while working for the charitable organization Doctors Without Frontiers.²⁵⁹

The Supreme Court of Russia has rejected efforts by human rights groups to disallow the use of anonymous declarations in the work of the FSB.²⁶⁰ The court specifically said that the December 2000 FSB directive encouraging the use of such denunciations in investigations was entirely legal.

Foreign Intelligence

Speaking at a 21 December 1995 Moscow celebration of the 75th anniversary of the formation of the VChK-KGB-SVR, Primakov declared that NATO expansion would create a "security threat" for Russia. Primakov said that trying to understand the "true motives" of those who advocate NATO enlargement is a key task of the SVR and added his agency would seek to block the alliance's expansion while trying to establish good relations with former Cold War adversaries. Primakov said Russian policy should seek to prevent the emergence of a "global hegemony" by the United States.

Primakov also stressed the importance of combating the threats of ethnic-national conflicts and terrorism to Russian territorial integrity and national security.

Important areas of SVR intelligence activity include possible scientific breakthroughs, which might radically change the Russian security situation, as well as determining those areas in which the actions of foreign states' special services and organizations might damage Russian interests.

The SVR contact with various intelligence and counterintelligence services of foreign states is one of the agency's fastest growing areas of activity. The SVR maintains working contacts and collaborates with several dozen special services in other countries. This includes work on nonproliferation of weapons of mass destruction; combating terrorism, the drug trade, organized crime, money laundering, and illicit arms trade; and the search for and release of hostages, as well as citizens of Russia and CIS countries, who are reported missing.

Collaboration includes the exchange of intelligence information, assistance in training of personnel, and material and technical assistance. The SVR also has reportedly concluded formal cooperation agreements with the intelligence services of several former Soviet republics, including Azerbaijan and Belarus, which cover gathering and sharing intelligence.

An agreement on intelligence cooperation between Russia and China was signed in Beijing at the end of the summer of 1992. It envisaged the restoration of the cooperation in the area of intelligence, which had been cut off in 1959. This secret treaty covered the activities of the GRU and the SVR, which are cooperating with the Chinese People's Liberation Army's Military Intelligence Directorate.

Although the SVR [along with other agencies] is involved in industrial espionage, there are signs that the data being collected by Russian intelligence agencies are not being used effectively. In a 7 February 1996 Security Council meeting—which included FSB Director Barsukov and SVR Director Trubnikov—President Yeltsin ordered top state officials to close the technology gap with the West by more efficiently using industrial intelligence. Yeltsin complained that less than 25 percent of the information collected by Russian spies abroad was used in Russia, even though he claimed information was derived directly from foreign blueprints and manuals.

SVR economic intelligence activities includes the identification of both threats to Russian interests as well as emerging opportunities, such as advantageous market trends for particular types of commodities and raw materials. Priority is attached to ensuring balanced development of relations with foreign countries in such spheres as currency and finance, export and import transactions for strategic raw materials, and in the high-technology sphere. The SVR is frequently commissioned to ascertain the business reputation and real potential of foreign firms and individual dealers who intend to establish business relations with Russian state organizations. It also seeks to identify foreign firms attempting to persuade certain Russian partners to conclude illegal export deals and to track Russian capital going abroad.

In addition to the economic, scientific, and technical focus of collections efforts noted above, human intelligence (HUMINT) collection against American intelligence agencies also has been ongoing, as exemplified by the 1996 arrests of FBI agent Earl Edwin Pitts and CIA officer Harold James Nicholson. The end of 1996 was also marked

by the case of former SVR Col. Vladimir Galkin, provoking a noisy scandal that added tension to Russian-American relations and relations between the SVR and the CIA.²⁶¹

President Putin secretly directed the SVR and the GRU to increase their activities in the United States. Putin's 2001 directive included orders to clarify the political context of statements by several members of the new US administration and to track developments related to NMD. Russian Security Council Secretary Ivanov is to coordinate this effort.²⁶²

The SVR also complained that Foreign Minister Igor Ivanov was not doing enough to support SVR stations at Russian embassies abroad. The SVR believed this lack of support by Russian diplomats led to the intelligence failures in the United States.²⁶³

Russian Spies Caught

Shigehiro Hagisaki

The most spectacular spy scandal to hit Japan in 20 years occurred on 8 September 2000 when the Tokyo Metropolitan Police arrested Shigehiro Hagisaki, formerly a lieutenant commander with the Maritime Self-Defense Force, as he was sitting in a restaurant with his Soviet embassy contact, Captain Viktor Bogatenkov. Hagisaki had just handed Bogatenkov copies of a classified training manual used by senior Maritime Self-Defense Force offices and papers regarding plans for military communications systems when the police made their move.

The arrest came just days after Russian President Putin visited Japan. A Russian Embassy official denounced the arrest, saying it “was a provocation aimed at reducing bilateral relations . . . ”

The police had been watching Hagisaki since September 1999 when he first began meeting with Bogatenkov at military events. At the time, Hagisaki was chief navigator for a Japanese naval escort ship. Since their initial meeting in September 1999, the two men met about 10 times.

A graduate of Japan's military academy, Hagisaki served on destroyers and submarines before being posted to the Defense Institute in March 2000. He worked there as a specialist on the Russian Navy.

In his apartment and at his office, police discovered classified documents on the movements of US naval forces in Japan, including US submarines.

Bogatenkov, a GRU officer, departed Japan the next day. The police said that Bogatenkov, who spoke fluent Japanese, paid for thousands of dollars worth of food and drink in return for copies of documents marked "Secret" and "Caution," which Hagisaki secretly removed from the Defense Institute.

On 27 November 2000, Hagisaki pled guilty to charges that he leaked defense secrets, including information about US Navy units in Japan, to Bogatenkov. He was cashiered from the military.

On 7 March 2001, Hagisaki was sentenced to 10 months in prison.

The Hagisaki case is the most high-profiled case since 1980 when a military attache at the Soviet Embassy in Japan obtained copies of a military monthly bulletin and official telegrams related to the Foreign Ministry. A retired Japanese major general, who obtained the information from several former army officers who had served under him, passed them to the Soviet attache.

Poland Arrests Russian Spies

In mid-1999, the Polish security services arrested three Polish military intelligence officers for espionage on behalf of Russia. All three held high posts in Polish counterintelligence up to 1993. One officer, identified only as Lt. Col. Czeslau W., was the former head of military counterintelligence in Lodz. He was arrested in June 1999.

In May 2000, Czeslau W. was found guilty of supplying the KGB with secret information on Polish counterintelligence and sentenced to four years in prison. However, on 29 August, the Polish

Supreme Court revoked the prison sentence, ordered the release of Czeslau and returned the case back to the court. As a condition of his released, Czeslau is to be under police supervision and is not allowed to leave Poland.

Another officer arrested was identified as Col. Zbigniew H. He has not been tried as yet. The third individual has not been identified.

Poland Expels Russians

On 20 January 2000, Poland declared nine Russian Embassy employees persona non grata. Polish Prime Minister Jerzy Buzek called the expulsions a great success for the Polish security service and the State Protection Office. Buzek's office claimed the Russians were targeting Polish economic, trade, and industrial information. In retaliation, Russia expelled nine Polish Embassy officials in Moscow for espionage.

Reaction to US Expulsion of Russian Diplomats

Russian Security Council Secretary Ivanov said in March 2001 that the tit-for-tat spy scandal would put an end for a while to "fruitful cooperation" between the Russian and American security services. Ivanov added he was concerned by what he called a trend in US policy to view Moscow as "a nuclear bogeyman" and then suggested that the Russians would be so stupid as to use 50 diplomats in the Hanssen case.²⁶⁴

Yuri Drozdev, the former chief of the KGB's Directorate S (Illegals), said that Washington's expulsion of 50 Russian embassy employees is "a stupid act aimed at undermining Russia's renewed assertiveness in foreign affairs." He said that Moscow should retaliate by expelling far more Americans, including those working at the NATO information center and in joint ventures.²⁶⁵

The American-Russian tit-for-tat expulsions caused England's Prime Minister Tony Blair to complained to Russian President Putin directly at their Stockholm

meeting about Russian spying, something British officials later denied. Simultaneously, the British Foreign Office said, “we are looking carefully as to whether the Russians have crossed the line. If we find that they have, we will do as the Americans did,” London newspapers reported.

Elsewhere, the German counterintelligence agency BundesVerfassungschutz concluded that in 2000, Russia increased the number of its intelligence officers working under diplomatic cover. In its annual report published at the agency website (<http://www.verfassungschutz.de>), German Interior Minister Otto Schily directly connected the increase to the rise of Putin in Moscow.

Russian Defections

Igor Dereichuk

The Russian Embassy in Panama informed local officials that cultural attache Igor Dereichuk disappeared in early March 2001. But Dereichuk’s relatives in Kiev said that he has told them that he simply does not want to work for the Russian Foreign Ministry any longer.²⁶⁶

Aleksandr Litvinenko

Aleksandr Litvinenko requested political asylum in the United Kingdom, saying that he feared the FSB may be seeking to kill him to prevent him from revealing information, including on last year’s apartment bombings in Moscow. Litvinenko gained notoriety in 1998 when he claimed that an FSB deputy department head had tasked him with killing Berezovskiy. He was fired from the FSB the following year.²⁶⁷ On 25 March 1999, Litvinenko was arrested and detained in Lefortovo Detention Center for eight months.

On 26 November the Moscow Military Garrison court ruled that the case against him be dropped for lack of evidence and that he be released from custody. But FSB officers arrested Litvinenko immediately after the acquittal—in the actual courtroom. On 16 December the same court freed him again—this time with a guarantee that he would not leave Russia.

After his release, Litvinenko, his wife, and small child fled to Turkey via the Ukraine. From Turkey he received assistance from Alexander Goldfarb, head of the Moscow office of the New York Institute of Public Health, who took the Litvinenko family to Britain.²⁶⁸

Unidentified SVR Officer

A SVR officer defected from the Russian Embassy in Ottawa at the end of 2000. He was part of the SVR directorate for external counterintelligence.²⁶⁹

Sergei Tretyakov

Sergei Tretyakov defected from the Russian mission to the UN in October 2000. He held the rank of colonel and was second in command of the SVR station in New York. The Russian media speculated that Tretyakov might have exposed Russian spy Hanssen because he probably had access to information about Hanssen.

The GRU

In April 2001, Putin shifted Ivanov from the Security Council to the Defense Ministry. Ivanov planned a clean sweep of the Ministry, but several senior officials had offered to resign even before Ivanov asked. The then chief of the general staff, Anatolii Kvashnin, was reported moving to the Security Council, and two Yeltsin holdovers, Deputy Defense Minister Valeriy Manilov and Colonel General Leonid Ivashov, were to follow.²⁷⁰

In the GRU, Ivanov reshuffled its leadership by replacing director Valentin Korabelnikov with someone from the SVR. The GRU was the least changed since Soviet times, and while Ivanov is known to have great respect for it, he wanted his own man in charge.²⁷¹

Lt. Gen. Valeriy Volodin, the chief of the GRU’s Electronic Warfare Directorate, said that his service is well prepared for penetrating the information systems of enemies but suffers from some problems because of technological shortcomings.²⁷²

Endnotes

¹ Kagedan, Allan, "Succeeding the KGB: Russian Internal Security in Transition," *Commentary No. 24*, Canadian Security and Intelligence Service, June 1992.

² ITAR-TASS, 30 June 1995.

³ *Sobraniye Zakonodatelstva Rossiyskoy Federatsii*, 31 July 1995, page 5781.

⁴ Interfax, 24 July 1995.

⁵ *Moscow News*, 28 July-3 August 1995).

⁶ *Komsomolskaya Pravda*, 22 August 1995; Moskovskiy Komsomolets, 11 October 1995.

⁷ Moskovskiy Komsomolets, 5 October 1994.

⁸ *Izvestiya*, 7 December 1994.

⁹ Moskovskiy Komsomolets, 31 December 1994.

¹⁰ Moskovskiy Komsomolets, 23 November 1995.

¹¹ Interfax, 24 July 1995; *Rossiyskaya Gazeta*, 27 July 1995.

¹² *Sobraniye*, 31 July, page 5781.

¹³ Moskovskiy Komsomolets, 5 and 25 July 1995).

¹⁴ *Moscow News*, 28 July-3 August 1995.

¹⁵ *Komsomolskaya Pravda*, 22 August 1995.

¹⁶ Moskovskiy Komsomolets, 3 November 1994.

¹⁷ *Komfflersant-Daily*, 25 July 1995.

¹⁸ *Segodnya*, 26 July 1995.

¹⁹ Interfax, 24 July 1995.

²⁰ Not further identified.

²¹ RIA, 20 September 1995.

²² Moskovskiy Komsomolets, 19 September 1995.

²³ Moskovskiy Komsomolets, 5 July 1995.

²⁴ ITAR-TASS, 28 September 1995; Moskovskiy Komsomolets, 4, 6, 11 October 1995.

²⁵ Moskovskiy Komsomolets, 4 October 1995.

²⁶ Ibid.

²⁷ *Obshchaya Gazeta*, 17-23 August 1995.

²⁸ *Segodnya*, 12 August 1995.

²⁹ *Nezavisimaya Gazeta*, 3 November 1995.

³⁰ The FSB Antiterrorist Center is a special unit, formed in 1995 that encompassed FSB combat and operational counterterrorist units.

³¹ *Sobraniye*, 18 September 1995, page 6880; *Segodnya*, 15 September 1995; *Izvestiya*, 16 September 1995.

³² ORT, 19 September 1995; *Segodnya*, *Rossiyskiye Vesti*, 7 December 1995.

³³ Interfax, 10 November 1995; *Segodnya*, 11 November 1995; *Rossiyskaya Gazeta*, 14 November 1995.

³⁴ The list of directorates and other subdivisions of the FSB in the 23 June FSB statute included no unit for foreign intelligence (*Sobraniye*, 26 June, page 4684).

³⁵ Interfax, 8 December 1995; *Segodnya*, 9 December 1995.

³⁶ *Sobraniye*, 21 August 1995, page 6475.

³⁷ *Komsomolskaya Pravda*, 20 September 1995.

³⁸ ITAR-TASS, 19 September 1995; Moskovskiy Komsomolets, 11 October 1995.

³⁹ *Komsomolskaya Pravda*, 22 August 1995; Moskovskiy Komsomolets, 11 October 1995.

⁴⁰ ITAR-TASS, 9 November 1995; *Rossiyskaya Vesti*, 10 November 1995.

⁴¹ The State Technical Commission was created by a 5 January 1992 Yeltsin edict to "protect information constituting state and workplace secrets in political, economic, scientific, technical, military, and other fields." It was formed out of the former USSR State Commission for Countering Foreign Technical Intelligence and placed "under" Yeltsin, with Yashin as chairman. See *Rossiyskaya Gazeta*, 10 January 1992. The 63-year-old Yashin was a deputy defense minister, army general, and doctor of technical sciences. The members of the Commission included 19 ministers and deputy ministers from the Ministries of Security, Economy, Foreign Affairs, Defense, and Science and the Academy of Sciences. See *Rossiya*, 21 April 1993.

⁴² ITAR-TASS, 9 November 1995.

⁴³ Moskovskiy Komsomolets, 10 November 1995; *Komsomolskaya Pravda*, 11 November 1995.

⁴⁴ *Nezavisimaya Gazeta* on 10 January 1995 published an FSK document warning of the danger of foreigners gathering information, and several papers published excerpts from a memo by Deputy Premier Vladimir Polevanov, citing data from the FSK that foreign businesses were secretly acquiring control over Russian enterprises and "subverting" Russia's defense.

⁴⁵ ITAR-TASS, 24 October 1995.

⁴⁶ *Rossiyskaya Gazeta*, 21 September 1993.

⁴⁷ *Rossiyskaya Gazeta*, 1 April 1994.

⁴⁸ *Rossiyskaya Gazeta*, 1 March 1995.

⁴⁹ *Sobraniye Zakonodatelstva Rossiyskoy Federatsii*, 11 September 1995, page 6782.

⁵⁰ *Rossiyskaya Gazeta*, 4 November 1994.

⁵¹ *Rossiyskaya Gazeta*, 7 April 1993.

⁵² *Sobraniye*, 26 June 1995, page 4678.

⁵³ ITAR-TASS, 10 March 1994.

⁵⁴ *Krasnaya Zvezda*, 12 August 1995; *Izvestiya*, 2 November 1995.

⁵⁵ *Krasnaya Zvezda*, 12 August 1995.

⁵⁶ *Izvestiya*, 2 November 1995.

⁵⁷ *Rossiyskaya Gazeta*, 4 November 1994.

⁵⁸ *Sobraniye*, 20 February 1995, pages 1222-24.

⁵⁹ *Rossiyskaya Gazeta*, 1 March 1995.

⁶⁰ *Rossiyskaya Gazeta*, 5 May 1995.

-
- ⁶¹ *Sobraniye*, 10 April 1995, page 2328.
- ⁶² *Sobraniye*, 26 June 1995, page 4678.
- ⁶³ *Sobraniye*, 3 July 1995, pages 4892-97; *Moskovskiy Komsomolets*, 1 July 1995; *Rossiyskiye Vesti*, 5 July 1995.
- ⁶⁴ *Sobraniye*, 14 August 1995, pages 6132-6145.
- ⁶⁵ *Moskovskiy Komsomolets*, 11 October 1995.
- ⁶⁶ *Sobraniye Aktov Prezidenta I Pravitelstva Rossiyskoy Federatsii*, No. 26, 26 June 1995.
- ⁶⁷ *Rossiyskaya Gazeta*, 18 August 1995.
- ⁶⁸ *Obshchaya Gazeta*, No. 40, 5-11 October 1995.
- ⁶⁹ *Rossiyskaya Gazeta*, 8 February 1992.
- ⁷⁰ According to Korzhakov in a 16 November 1994 *Nezavisimaya Gazeta* interview.
- ⁷¹ ITAR-TASS, 29 July 1995.
- ⁷² ITAR-TASS, 29 July 1995.
- ⁷³ *Rossiyskaya Gazeta*, 1 August 1995.
- ⁷⁴ *Izvestiya*, *Rossiyskiye Vesti*, 8 July 1995.
- ⁷⁵ *Rossiyskaya Gazeta*, 7 July 1995.
- ⁷⁶ *Radio Rossii*, 20 July 1995; ITAR-TASS, 24 July 1995.
- ⁷⁷ *Rossiyskaya Gazeta*, 6 July 1995.
- ⁷⁸ ITAR-TASS, Interfax, 20 June 1996.
- ⁷⁹ Ekho Moskv, 19 June 1996, said it was at FSB headquarters.
- ⁸⁰ Chubays in his 20 June 1996 press conference specified that Lisovskiy was not a member of the president's campaign staff "but has played an important role" in directing "several key projects within the presidential campaign. See ORT, 20 June 1996. According to 21 June 1996 *Segodnya*, Chubays called the two "key participants in Boris Yeltsin's election campaign."
- ⁸¹ Ekho Moskv, 20 June 1996.
- ⁸² Soskovets had been replaced as head of the president's campaign staff in March 1996.
- ⁸³ ITAR-TASS, 20 June 1996.
- ⁸⁴ RTV, 20 June 1996.
- ⁸⁵ ORT, 20 June 1996.
- ⁸⁶ Interfax, 20 June 1996.
- ⁸⁷ ITAR-TASS, 20 June 1996.
- ⁸⁸ Soskovets appointment was based on Korzhakov's recommendation, according to a 20 June 1996 ITAR-TASS report.
- ⁸⁹ *Izvestiya*, 21 June 1996.
- ⁹⁰ *Izvestiya*, 21 June 1996.
- ⁹¹ ORT, 20 June 1996.
- ⁹² ITAR-TASS, 20 June 1996; *Izvestiya*, 21 June 1996.
- ⁹³ NTV, 20 June 1996.
- ⁹⁴ *Segodnya*, 21 June 1996.
- ⁹⁵ ORT, 20 June 1996.
- ⁹⁶ *Radio Mayak*, 20 June 1996.
- ⁹⁷ *Izvestiya*, 21 June 1996.
- ⁹⁸ *Izvestiya*, 21 June 1996.
- ⁹⁹ *Segodnya Izvestiya*, 21 June 1996; ORT, 20 June 1996.
- ¹⁰⁰ NTV, 19 June 1996.
- ¹⁰¹ Interfax, 20 June 1996.
- ¹⁰² *Izvestiya*, 21 June 1996.
- ¹⁰³ ORT, 20 June 1996; *Izvestiya*, 21 June 1996.
- ¹⁰⁴ Interfax, 22 June 1996.
- ¹⁰⁵ ITAR-TASS, 20 June 1996.
- ¹⁰⁶ For example, Korzhakov blocked Ilyushin's access to Yeltsin during the president's October hospitalization and appeared to get his ally Nikolay Yegorov named leader of the president's Administration in January 1996, probably impinging on Ilyushin's influence.
- ¹⁰⁷ Interfax, 20 June 1996.
- ¹⁰⁸ *Izvestiya*, 21 June 1996.
- ¹⁰⁹ *Segodnya*, 21 June 1996.
- ¹¹⁰ *Izvestiya*, 21 June 1996.
- ¹¹¹ ITAR-TASS, 20 June 1996.
- ¹¹² ORT, 20 June 1996.
- ¹¹³ According to a 20 June ITAR-TASS report at 0929 GMT and to the 21 June *Nezavisimaya Gazeta*, Yeltsin's talk with Chernomyrdin took place after the Security Council meeting, rather than before.
- ¹¹⁴ ITAR-TASS, 20 June 1996.
- ¹¹⁵ NTV, 20 June 1996.
- ¹¹⁶ *Rossiyskaya Gazeta*, 21 June 1996.
- ¹¹⁷ Interfax, 20 June 1996.
- ¹¹⁸ *Nezavisimaya Gazeta*, 21 June 1996.
- ¹¹⁹ *Rossiyskaya Gazeta*, 21 June 1996; *Nezavisimaya Gazeta*, 21 June 1996; ITAR-TASS, 20 June 1996.
- ¹²⁰ *Rossiyskaya Gazeta*, 21 June 1996; *Nezavisimaya Gazeta*, 21 June 1996.
- ¹²¹ RTV, 20 June 1996.
- ¹²² Interfax, 20 June 1996.
- ¹²³ NTV, 20 June 1996.
- ¹²⁴ *Segodnya*, 21 June 1996.
- ¹²⁵ Interfax, 20 June 1996.
- ¹²⁶ *Segodnya*, 21 June 1996; *Nezavisimaya Gazeta*, 21 June 1996.
- ¹²⁷ RTV, 20 June 1996.
- ¹²⁸ ORT, 20 June 1996.
- ¹²⁹ *Segodnya*, 21 June 1996; *Nezavisimaya Gazeta*, 21 June 1996.
- ¹³⁰ *Izvestiya*, 21 June 1996.
- ¹³¹ ITAR-TASS, 20 June 1996.
- ¹³² *Komsomolskaya Pravda*, 21 June 1996.
- ¹³³ Yeltsin renamed the Main Protection Director (GUO)

the Federal Protection Service (Federalnaya Sluzhba Okhrany—FSO). He named GUO Director Krapivin its chief in a 19 June 1996 edict. See *Rossiyskaya Gazeta*, 25 June 1996. He then merged the FSO and SBP into a single State Protection Service (Sluzhba Gosudarstvennoy Okhrany—SGO) in a 2 July 1996 edict (see Interfax, 4 July 1996) with Krapivin acting chief (see Moskovskiy Komsomolets, 5 July 1996).

¹³⁴ US Department of State statement, 15 August 1995.

¹³⁵ Interfax, 3 August 1998; Russkiy Telegraf, 28 July 1998.

¹³⁶ *Nezavisimaya Gazeta*, 28 July 1998.

¹³⁷ *Komsomolskaya Pravda*, 28 July 1998.

¹³⁸ Interfax, 3 August 1998.

¹³⁹ *Voice of Russia*, radio report, 7 August 2000.

¹⁴⁰ *Literaturnaya Gazeta*, No. 31.

¹⁴¹ See FBIS Media Analysis, “Russia: Abramovich Now Top Oligarch, but His Goals, Intentions Remain a Puzzle,” 2 November 2000.

¹⁴² *Versiya*, 24 April, 8 June, and 7 November 2001.

¹⁴³ *Ibid.*, 25 May 2001.

¹⁴⁴ See FBIS Media Analysis, “Russia: ‘Black Hole’ in Economy Fended Off, but Real Reform Remains Elusive,” 24 April 2001.

¹⁴⁵ See FBIS Media Analysis, “Russia: Expanded Authority of Minister of Natural Resources Allows Kremlin to Court Foreign Investment Yet Favor Domestic Developers,” 14 November 2000.

¹⁴⁶ NTV, 16 June 2001, Kommersant, 18 June 2001.

¹⁴⁷ <Grani.ru>, 8 June and 18 June 2001.

¹⁴⁸ Moskovskiy Komsomolets, 18 June 2001.

¹⁴⁹ <Grani.ru>, 18 June 2001.

¹⁵⁰ Grani.ru, 18 June 2001.

¹⁵¹ For more information on Levayev and Rudakov, see FBIS Media Analyses, “Russia: Émigré Diamond War Tycoon Creates Transnational ‘Verticl Cartel’,” 21 June 2000; “Russia: ‘Diamond War’ Reaches Kremlin, Could Awaken Putin’s ‘Ghosts’,” 13 February 2001; “Russia: Émigré Tycoon Said To Use Kremlin To Settle Scores With Gusinsky,” 22 February 2001; and “Russia: Hard-Pressed Diamond Monopoly Names Old Putin Foe as Point Man,” 2 April 2001.

¹⁵² ORT, 19 June 2001.

¹⁵³ *Nezavisimaya Gazeta*, 19 June 2001. This newspaper was for some time considered the mouthpiece of oligarch Boris Berezovskiy but then began to hew to a more pro-Kremlin line, especially as Berezovskiy fell out with the Kremlin. Editor-in-chief Vitaliy Tretyakov, who often boasted of his editorial independence,

resigned on 6 June 2001 because of “political differences with owner Berezovskiy.”

¹⁵⁴ *Ibid.*

¹⁵⁵ Grani.ru, 18 June 2001.

¹⁵⁶ <Utro.ru>, 13 June 2001.

¹⁵⁷ *Rossiyskaya Gazeta*, 19 June 2001.

¹⁵⁸ Moskovskiy Komsomolets, 1 June 2001.

¹⁵⁹ Kommersant-Dengi, 6 June 2001.

¹⁶⁰ Kommersant-Dengi, 6 June 2001; Grani.ru, 8 June 2001; Rossiya, 5 June 2001; Gazeta.ru, 9 April 2001.

¹⁶¹ Profil, 4 June 2001; Kommersant-Dengi, 6 June 2001.

¹⁶² Smi.ru, 25 May 2001.

¹⁶³ Apn.ru, 18 June 2001.

¹⁶⁴ For more information on Zaostrovtssev, see FBIS Media Analyses, “Russia: Black Hole in Economy Fended Off, but Real Reform Remains Elusive,” 24 April 2001; and “Russia: Growing Pressure on Procurator Bolsters Chances of ‘Mini-KGB’s Man,” 4 May 2001.

¹⁶⁵ SSR *Rossiyskaya Gazeta*, 28 November 1992, makes reference to “former head of Gokhran SSR Kozlov.” Kommersant-Dengi, 20 June 2001.

¹⁶⁶ Apn.ru, 25 June 2001.

¹⁶⁷ Trubnikov’s appointment was reported both in *Segodnya* and *Kommersant Daily* on 29 June 2000.

¹⁶⁸ A longtime veteran of the KGB, Mylnikov comes from St. Petersburg. During the Soviet period, he worked in the KGB’s 5th Chief Directorate, which was responsible for combating “hostile ideologies” and tracking down dissidents. Later he moved to Ekaterinburg and Stavropol. When Putin was still FSB director, he recreated the directorate for the protection of the constitutional order and named Mylnikov to be deputy chief. As deputy, Mylnikov played an active role in both Chechen campaigns and adopted a style that “Kommersant Daily” said marked him as “a real Andropovite.”

¹⁶⁹ Shebarshin’s comments appeared in *Rossiyskaya Gazeta* on 26 October 2000.

¹⁷⁰ RIA-Novosti, 1 November 2000.

¹⁷¹ Profil, no.44.

¹⁷² ITAR-TASS, 13 November 2000.

¹⁷³ *Vedimosti*, 15 November 2000.

¹⁷⁴ Grani.ru, 3 May 2001.

¹⁷⁵ Novye Izvestiya, 7 June 2001.

¹⁷⁶ Komok, 4 June 2001.

¹⁷⁷ Grani.ru, 18 June 2001.

¹⁷⁸ Strana.ru, 19 June 2001.

¹⁷⁹ *Segodnya*, 4 July 2000.

¹⁸⁰ *Segodnya*, 10 January 2001.

- ¹⁸¹ Hoffman, David, "In Russia, Spies Come in From Cold," *The Washington Post*, 8 December 2000.
- ¹⁸² RFE/RL Newswire, 11 May 2000.
- ¹⁸³ CPJ press release, 15 May 2000.
- ¹⁸⁴ FRE/RL Newswire, 12 May 2000.
- ¹⁸⁵ Moskovskii Komsomolets, 13 May 2000.
- ¹⁸⁶ In an interview with Ekho Moskvyy, 12 May 2000.
- ¹⁸⁷ RFE/RL Newswire, 16 May 2000.
- ¹⁸⁸ *Kommersant-Daily*, 3 June 2000.
- ¹⁸⁹ *RIA-Novosti*, 18 October 2000.
- ¹⁹⁰ *Versiya*, No. 20.
- ¹⁹¹ *Kommersant*, 6 September 2000.
- ¹⁹² See "Radio Free Europe/PL Security Watch," No. 3, 7 August 2000.
- ¹⁹³ *Vek*, No. 44, November 2000.
- ¹⁹⁴ *Segodnya*, 11 November 2000.
- ¹⁹⁵ Glasnost Defense Foundation Information Sector, 17 November 2000.
- ¹⁹⁶ *Gazeta.ru*, 30 April 2001.
- ¹⁹⁷ Copyright© 2000. RFE/RL, Inc. Reprinted with the permission of Radio Free Europe/Radio Liberty, 1201 Connecticut Avenue, NW, Washington, DC 20036. www.rferl.org. Victor Yasmann authored the article.
- ¹⁹⁸ Copyright© 2000. RFE/RL, Inc. Reprinted with the permission of Radio Free Europe/Radio Liberty, 1201 Connecticut Avenue, NW, Washington, DC 20036. www.rferl.org. Victor Yasmann authored the article.
- ¹⁹⁹ *Novye Izvestiya*, 29 November 2000.
- ²⁰⁰ *Izvestiya*, 1 June 2001.
- ²⁰¹ *Vremya MN*, 1 June 2001.
- ²⁰² *Argumenty I fakty*, No.22.
- ²⁰³ *Moscow Times*, 7 June 2001.
- ²⁰⁴ *Moskovskiy Komsomolets*, 12 January 2001.
- ²⁰⁵ *RIA-Novosti*, 4 June 2001.
- ²⁰⁶ Vladimir Lenin created the first Soviet secret police, the Extraordinary Commission or Cheka, just weeks after the October 1917 revolution, which brought the Communists to power in the Soviet Union. Joseph Stalin created a holiday called "the Day of the Chekist" to honor those who serve in the Soviet/Russian intelligence services. Officers in Moscow's variously named intelligence agencies proudly called themselves "Chekists" in honor of that first name.
- ²⁰⁷ See TASS, 20 December 2000; *Izvestiya*, 20 December 2000; and *Nezavisimaya Gazeta*, 20 December 2000.
- ²⁰⁸ *Izvestiya*, 27 February 2001.
- ²⁰⁹ *Christian Science Monitor*, 13 June 2001.
- ²¹⁰ *Nezavisimoe voennoe obozrenie*, No. 16, 31 April 2001.
- ²¹¹ Lunev, Col. Stanislav, "Influences of Russia's Special Services Increase," NewsMax.com, 16 July 2001.
- ²¹² *Strana.ru*, 22 February 2001.
- ²¹³ *ITAR-TASS*, 19 June 2001.
- ²¹⁴ *Vremya MN*, 19 April 2001.
- ²¹⁵ *Interfax*, 19 April 2001.
- ²¹⁶ Vitaliy Potapov, "Navy Institute Employee Was 'Working got CIA,'" *TRUD*, 17 September 1996.
- ²¹⁷ Oleg Odnokolenko, "How Much Do People Sell the Motherland For"? *Segodnya*, 10 February 1999.
- ²¹⁸ *RIA-Novosti*, 16 January 2001.
- ²¹⁹ *Ekho Moskvyy*, 8 March 2001.
- ²²⁰ *Moscow Komsomolskaya Pravda*, 20 December 2000.
- ²²¹ *Interfax*, 23 April 2001.
- ²²² *Interfax*, 28 May 1999.
- ²²³ *Ibid.*
- ²²⁴ *Voice of America*, 8 February 1999.
- ²²⁵ Yevgeniya Lents, "Experts Rule Protocol in Pasko Spy Case Forged," *Itar-Tass*, 23 June 1999.
- ²²⁶ *Ekho Moskvyy*, 21 November 2000.
- ²²⁷ *NTV*, 23 July 2001.
- ²²⁸ *Interfax*, 24 August 2000.
- ²²⁹ *Izvestiya*, 10 August 2000.
- ²³⁰ *ORT*, 20 September 2000.
- ²³¹ *RIA-Novosti*, 27 September 2000.
- ²³² Michale Steen, "Ailing U.S. Suspect Attends Russian Spy Hearing," *Reuters*, 2 November 2000.
- ²³³ *Segodnya*, 27 October 2000.
- ²³⁴ *ORT*, 15 November 2000.
- ²³⁵ Sharon La Franiere, "American Denies Buying Secrets," *The Washington Post*, 26 October 2000, p. A29.
- ²³⁶ *Rossiyskaya Gazeta*, 10 November 2000.
- ²³⁷ *Interfax*, 21 November 2000.
- ²³⁸ *RIA-Novosti*, 6 December 2000.
- ²³⁹ *NTV*, 6 and 7 December 2000.
- ²⁴⁰ *Segodnya*, 7 December 2000.
- ²⁴¹ *Moscow Times*, 7 December 2000.
- ²⁴² *ORT television*, 6 December 2000.
- ²⁴³ John Mintz, "Unseen Perils in a Russian Squall," *The Washington Post*, 3 January 2001, p. A01.
- ²⁴⁴ *Moscow Komsomolskaya Pravda*, 20 December 2000.
- ²⁴⁵ Source: Keston Institute <http://www.keston.org>.
- ²⁴⁶ Aleksandr Khinshteyn, "Defense Industry Sleepy-Heads and FSK's Watchful Men," *Moskovskiy Komsomolets*, 15 May 1993, p. 3.
- ²⁴⁷ Radio Free Europe newswire, 19 June 2000.
- ²⁴⁸ *Vremya novostei*, 6 September 2000.

²⁴⁹ See Radio Free Europe/RL Security Watch, Vol. 2, No.8.

²⁵⁰ Interfax, 30 July 2001.

²⁵¹ Moscow Interfax, 8 August 2001.

²⁵² Pravda.ru, 11 June 2001, which cited *Vremya Novostei*.

²⁵³ Ekho Moskvyy radio Web site, www.echo.msk.ru, 13 June 2001.

²⁵⁴ Regions.ru, 13 June 2001.

²⁵⁵ Interfax, 7 June 2001.

²⁵⁶ *Nezavisimaya Gazeta*, 14 March 2001.

²⁵⁷ *Gazeta.ru*, 24 July 2000.

²⁵⁸ Interfax, 18 May 2001.

²⁵⁹ Regions.ru, 27 April 2001.

²⁶⁰ RIA-Novosti, 24 April 2001.

²⁶¹ Andrey Poleshchuk, "Interview With SVR Director Vyacheslav Trubnikov," *Nezavisimaya Gazeta*, 18 December 1996, pp. 1-2; "Yeltsin Admits Russians Engage in Economic Espionage, Counterintelligence News and Digest, National Counterintelligence Center, Vol. 1, March 1996; Jeff Stein, "I, Spy Cold Warriors No More, Russian Spies Languish in Irrelevance."

²⁶² *Rossiya*, 15 February 2001.

²⁶³ *Obshchaya Gazeta*, 30 April 2001.

²⁶⁴ ITAR-TASS, 26 March 2001.

²⁶⁵ *Vremya Novostei*, 23 March 2001.

²⁶⁶ ITAR-TASS, 15 March 2001.

²⁶⁷ RFE/RL Newsline, 3 November 2000.

²⁶⁸ Moscow *Izvestiya*, 16 May 2001.

²⁶⁹ *Moskovskiy Komsomolets*, 7 March 2001.

²⁷⁰ *Grani.ru*, 5 April 2001.

²⁷¹ *Versiya*, 2 April 2001, and *Zhizn*, 4 April 2001.

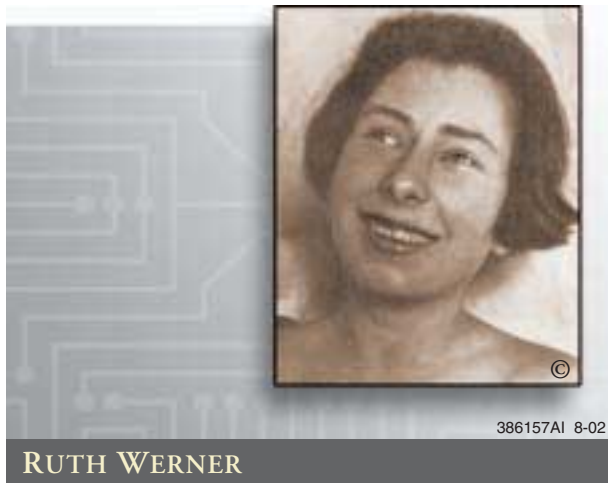
²⁷² *Krasnaya Zvezda*, 14 April 2001.

Vladimir Semichastny

Vladimir Semichastny, KGB chief from 1961 to 1967, died on 12 January 2001 in Moscow at the age of 78. Semichastny, born 1 January 1924, was first secretary of the Central Committee of the Komsomol from 1958 to 1959. He reportedly played an active role in the ouster of Nikita Khrushchev as first secretary of the Communist Party of the Soviet Union's Central Committee and chairman of the Council of Ministers. In 1961 he became KGB chairman when he was only 37 years old, but his short time in power had a mixed record. He was responsible for persecuting Russian dissidents Andrei Sinyavsky, Yuli Daniel, Boris Pasternak, and Josef Brodsky. Conversely, he not only helped catch CIA agent Oleg Penkovskiy, but also organized several "successful penetration operations" against Western intelligence services. In 1967, Soviet leader Leonid Brezhnev dismissed Semichastny from the KGB and demoted him to first deputy chairman of the Council of Ministers of the Ukrainian SSR.

Ruth Werner

Ruth Werner, age 93, a lifelong communist who channeled atomic bomb secrets to the Soviets during World War II and handled some of Moscow's most notorious spies, died in July in Berlin. The reformed communist Party of Democratic Socialism (PDS), of which she was a member, announced her death.



Werner, who operated under the codename Sonya, gained the rank of colonel in the Red Army. As a Soviet spy in United Kingdom in the 1940s, Werner was a contact for Klaus Fuchs, a German-born scientist who had been given political asylum. Fuchs had contacted the Russians to say that he was working with a team of British physicists in the United States to build an atomic bomb. He was put in touch with Werner, also German-born, who had been part of the Soviet spy network for many years.

On Fuchs' return to the United Kingdom in 1945, where he worked on a British bomb, Werner was again his link to Moscow, and through her he passed information that helped the Russians design their hydrogen bomb. She returned to East Germany in 1950, the year Fuchs was jailed for 14 years in the United Kingdom for passing atomic secrets to Moscow.

In retrospect, it was rare for a woman to make spying her career. The famous female spies of World War II, such as Violette Szabo, were quickly recruited, often for their language skills, and had short brave lives before they were caught and killed by the Germans. By contrast, Werner was an agent for some 20 years.

Trained as a bookseller, Werner joined the German Communist Party at age 19. In 1930, Soviet master spy Richard Sorge recruited Werner in China after she moved to Shanghai with her first husband who was working as an architect. She later saw action as a radio operator in Manchuria, Poland, and Switzerland before joining forces with Fuchs.

Werner later found fame as an author, publishing her memoirs, entitled *Sonya's Report*, in 1977. She also wrote a novel, *An Unusual Girl*, and a biography of anti-Nazi resistance fighter Olga Benario. Even after the collapse of East Germany, which led to the reunification of the two Germanys in 1990, she stayed active in the PDS. She had three children.

The Soviet Union was always looking for apprentice spies, and Werner seemed to be a promising candidate. She was a woman of leisure, well spoken, and had been given a good education by her middle-class parents. For her new spymasters, all this counted in her favor. They were short of posh ladies. They told her to watch her appearance and to wear a hat. Years later, she was able to meld easily into an Oxford community, her neighbors never suspecting that the nice Ruth Werner was the conduit of the West's treasured secrets to an enemy.

Patience was one of the strengths of the Soviet Union's immensely successful spy network under Stalin. "Always I was given plenty of time," Werner recalled.

CHAPTER 3

INTRODUCTION

In its 1998 report entitled “Technology Collection Trends in the US Defense Industry,” the Defense Security Agency (DSS) reported that the number of suspected industrial intelligence-gathering attempts against the US defense industry tripled since 1995. It also said that 37 nations were engaged in industrial espionage to gain information about US Department of Defense technology. In its 2001 report, the number of countries had grown to 63.

While the DSS study focused on foreign collection of classified or sensitive information on US weapons systems, emerging technologies with military applications, and related technical methods, intelligence collection against US economic, commercial, and proprietary information continues vigorously. This collection effort allows foreign nations and corporations to obtain shortcuts to industrial development and to improve their competitiveness against US corporations in the global marketplace.

At the same time, some foreign scientists and businessmen working with US firms or research institutes try to circumvent US laws to steal or illegally transfer embargoed American technology. There were several notable cases involving theft of American proprietary information. The first involved several Taiwanese nationals charged with allegedly trying to steal the secret formula for an anticancer drug made by the Bristol-Myers Squibb Company. Another was an Avery Dennison employee who supplied a Taiwanese firm some of his company’s most closely held secrets. In a third case, two Japanese stole genetic materials from Lerner Research Institute and made it available to an institute in Japan.

Spying by other nations within the United States also came to the surface during this period. The most notable of which was Cuba when it suffered setbacks with the arrest of seven members of its Wasp Spy network in Florida, its spy within the US Defense Intelligence Agency, and another in the US Customs Service. Five Americans were also arrested for selling or trying to sell US classified information to foreign intelligence services or nations.

Collection by the National Security Agency (NSA) came under the foreign microscope when the European Parliament alleged that NSA operates an international SIGINT collection effort—identified as ECHELON—that intercepts communications worldwide to provide economic intelligence to US corporations. On 5 July 2000, the European Parliament voted to launch a further investigation of ECHELON; the resultant draft report on ECHELON was made public on 18 May 2001. Maintaining that NSA operates in accordance with existing statutes and executive orders, senior US officials strongly disputed claims that intelligence agencies assist US corporations competing with foreign firms. They acknowledged, however, that intelligence agencies collect information regarding the use of bribery and other illegal efforts by foreign firms in competition with US corporations.

**Kai-Lo Hsu, Chester S. Ho,
and Jessica Chou**

Kai-Lo Hsu, Chester S. Ho, and Jessica Chou, all Taiwanese nationals, were charged with allegedly trying to steal the secret formula for Taxol, an anticancer drug made by the Bristol-Myers Squibb Company.¹ In October 1997, a Federal judge ordered prosecutors to turn over to the defendants and their lawyers the very documents the defendants are accused of trying to steal. The judge ruled that they needed the information to prepare their defense and that their right to a fair trial overrides the rights of a company to protect its trade secrets. Prosecutors appealed the ruling.

In a closely watched economic espionage case, the Third US Circuit Court of Appeals in Philadelphia ruled on 27 August 1998 that Federal prosecutors did not have to turn over trade secrets to defendants. The ruling reversed the lower court's decision.

The three-judge appeals panel said the defendants do not need to see the purported trade secrets because they can be guilty of conspiracy and attempted theft of trade secrets "even if the documents contained no confidential information at all." The appeals panel also said that the district judge's analysis was mistaken, since it was based on the belief that the defendants were charged with the actual theft of trade secrets. In fact, since they were charged with only an attempted theft, the defendants were not entitled to the documents because they were not an essential element of the prosecution's case.

The appellate court ordered the district judge to ensure that the trade secrets were edited out of the documents before they were turned over to the defendants.

On 31 March 1999, Kai-Lo Hsu, the technical director of the Yuen Foong Paper Co., Ltd., in Taipei, pleaded guilty to one count of conspiracy to acquire a trade secret. Under the plea, Hsu was to cooperate with Federal authorities who were investigating the extent of the conspiracy. In exchange for his cooperation, 10 other criminal charges against him were dropped, and a sentence below the 10-month prison term that was

recommended under sentencing guidelines will be encouraged. Hsu was released on \$1 million bail, awaiting sentencing.

Hsu was one of three people charged two years ago in an FBI sting operation. Also of the three, Jessica Chou, Yuen Foong Paper's business manager, is considered a fugitive by US authorities and is believed to be in Taiwan. The other defendant, Chester S. Ho—an MIT-trained biochemistry professor at two Taiwanese universities—was released last January after Federal prosecutors dismissed the charges against him.

According to the sentencing transcript produced in the US District Court for the Eastern District of Pennsylvania, Hsu was sentenced to two years' probation and fined \$10,000 on 13 July 1999 for conspiring to buy information regarding Taxol. The drug had earned the company almost \$1 billion in revenue.

The US Government took the position that, due to Hsu's cooperation, he was entitled to a departure under the sentencing guidelines. However, due to the seriousness of the offense, the prosecution argued that some period of incarceration was warranted in order to send a signal to those who are inclined to violate the Economic Espionage Act. Noting that technology has made the United States what it is today, the US Government also argued that it was important to prevent this kind of theft so that companies like Bristol-Myers Squibb will remain willing to take the risks and invest millions of dollars in developing technology that might or might not work. Despite this urging, the court sentenced Hsu to time served (14 days), two years of supervised release, and a \$10,000 fine.

A separate civil settlement was negotiated between Hsu's company, the Yuen Foong Paper Co., Ltd., in Taipei, and the US Government in the amount of \$300,000.

Endnote

¹ See *Counterintelligence Reader*, Volume III, pp. 414-415, for previous information on their arrest.

Theresa Squillacote, Kurt Stand, and James Clark: The Espionage Careers of Three Americans

Three people were arrested on 4 October 1997 and charged with spying for the former German Democratic Republic (GDR) and Russia in an espionage operation that began in 1972: the three coconspirators were Theresa Squillacote; her husband, Kurt Stand; and their friend James Clark. The three were described in court papers as Communist Party sympathizers who had met at the University of Wisconsin in Milwaukee during their student days in the 1970s.

Theresa Marie Squillacote, 39, was a senior staff attorney in the office of the Deputy Under Secretary of Defense for Acquisition Reform until January 1997. According to court papers, Squillacote got her job at the Pentagon after the German reunification in 1990 to gain access to government secrets. She had also sought a job at the White House Office of Management and Budget, which she had hoped to use as a springboard to a position at the National Security Council. Before her Pentagon assignment as a senior staff attorney, Squillacote had worked for the House Armed Services Committee.

Kurt Alan Stand, 42, was a regional representative of the International Union of Food, Agricultural, Hotel, Restaurant, Catering, Tobacco and Allied Workers Association. He was accused of starting his spy activities in 1973 when he was recruited by the GDR (East Germany) to develop spies in Washington. He recruited Squillacote around the time he married her in 1980.

James Michael Clark, 49, a private investigator from Falls Church, Virginia, once worked for a defense contractor at the Rocky Mountain Arsenal in Boulder, Colorado, where he had access to classified information on chemical warfare. Clark was accused of providing East Germany with US State Department documents concerning the Soviet leadership, Soviet nuclear doctrine, and military problems in the Soviet Bloc countries.

On 17 February 1998, Squillacote, Stand, and Clark were indicted by a federal grand jury on charges of conspiring to spy for the former GDR, the former Soviet Union, the Russian Federation, and South Africa. All three were held without bond until their trial on 20 July 1998. According to press reports, the US Justice Department reviewed the allegations to determine if special circumstances existed that warranted seeking the death penalty.

Kurt Stand's parents fled Germany for the United States during Hitler's regime. After the war, his family maintained contact with friends in eastern Germany, which became the German Democratic Republic in 1949. When Stand was approximately 18 years old, his father introduced him to Lothar Ziemer, an officer in charge of Section 3 of the Main Administration for Intelligence's (HVA) Department XI. HVA was the foreign intelligence arm of the Ministry of State Security (MfS),¹ East Germany's intelligence service. The primary mission of Department XI was the operational reconnaissance of North America. Its purpose was to acquire data of significance to the GDR that could not be acquired by legal means.

On an HVA codename agent data sheet, "Junior" is listed with file number "VX2207/73" and is listed as a source with direct access. The origin of the case is listed as "Agent in the West," and Junior is listed as having been recruited in 1972 in the GDR on an "ideological" basis by an MfS officer. Junior is listed as a married American male born in 1954 who lives in New York and is a trade union employee. Junior's target is listed as "Central trade union organization, USA, and direct contact at upper levels." He is deemed to be "reliable," and his means of communication are listed as one-way shortwave radio, accommodation addresses in the GRD and the West, cipher system, microdot, meetings in the West with his principal agent from the GDR, and international travel documents.

The HVA archival record for this file lists the case as having been opened on 1 October 1973 by Lothar Ziemer. An examination of a true name card in the file lists the name "Kurt Stand," born 5 November 1954 in New York. The date and place

of birth match those of Kurt Stand. Also in the file was another true name card in the name of “Alan David Jackson” with a date of birth identical to that of Stand. This was an alias on a British passport given to Stand for use in meeting with his GDR handler. The “Jackson” true name card had a stamp with the word “DOKUMENT” on it, which suggests that it was used on a document provided to an HVA agent.

In the early 1970s, Stand began working as an HVA agent responsible primarily for recruiting other agents. In 1976, Stand invited James Michael Clark, a college friend, to travel with him to Germany. Stand introduced Clark to an HVA operative, who introduced him to Ziemer. Ziemer invited Clark to join his organization, which he described as performing intelligence work on behalf of East Germany and other socialist countries, as well as for “liberation movements” in Asia, Latin America, and Africa. Clark agreed to join.

According to an HVA codename data sheet, “Jack” is listed with the file number “XV/43/77” and is listed as a source with direct access. The origin of the case is listed as “Agent in the West,” and Jack is listed as having been recruited in 1976 on an “ideological basis” by an MfS officer. Jack’s target is listed as “Ministry of Defense for a NATO country”. He is deemed “reliable,” and his means of communication are listed as one-way shortwave radio, accommodation addresses in the GDR and the West, a cipher system, code, microdot, contact with agent handler, and international travel documents and/or passport.

The HVA archival record for file number XV/43/77 lists the case as having been opened on 17 January 1977 by Lothar Ziemer, an HVA officer. A true name card listed under the same file number identified James Michael Clark, born 1 April 1948 in Lowell, Massachusetts. This is the correct date and place of birth of Clark.

A second true name card under the same file number lists a “Christopher Michael Glanz,” who was born 1 April 1949. This is believed to be an alias on a British passport that the HVA provided to Clark

for use in meeting with his HVA handlers. The Glanz true name, like the card on “Jackson” under Stand’s file, bears the same stamp with the word “DOKUMENT,” which suggests that it was the alias name used on a document provided to Clark.

Sometime between 1979 and 1981, Stand brought his wife, Theresa Squillacote, into the fold, and she too became what Ziemer described as an “informal collaborator.” At some point, Squillacote’s relationship with Ziemer became more than professional, and they had an affair that lasted until 1996.

Another HVA file, “XV/2207/73,” lists the codename “Resi,” who is described as a “Developmental agent,” recruited in 1981 in the GDR on an “ideological basis.” Resi is a married American female, born in 1957, who lives in Washington, DC, whose occupation is listed as “official lawyer.” Her target is described as “US Federal government.” She is deemed to be “trustworthy,” and her means of communication is listed as “met in West by principal agent from GDR.”

A true name card in the same file lists “Teresa Squillacote” with a birth date of 10 November 1957 in Chicago, Illinois. This is the same date and place of birth of Squillacote, who also was a lawyer with the National Labor Relations Board in Washington. Like Stand and Clark, there is another true name card with the name “Mary Teresa Miller,” with a date of birth identical to that of Squillacote. Like her two codefendants, the name was an alias on a British passport used by Squillacote to meet with her GDR handlers.

The HVA devoted substantial resources to the training of Squillacote, Stand, and Clark. They received training on detecting and avoiding surveillance, receiving and decoding messages sent by shortwave radio from Cuba, mailing and receiving packages through the use of accommodation addresses, using codewords and phrases, using a miniature camera to photograph documents, and removing classified markings from documents. HVA records indicate that the three conspirators together were paid more

than \$40,000 between 1985 and 1989, primarily as reimbursement for travel to many countries, including East Germany and Mexico, to meet with their handlers.

The HVA placed great value on these three agents and took numerous steps to protect their security. In their contacts with the three defendants, the HVA made extensive use of codenames and codewords to communicate tasking and operational instructions. For example, in the Operation “Junior” communications, the address frequently used by Squillacote and Stand to communicate with HVA headquarters was “Tante Klara,” and the intelligence service was referred to as the “family.” At various times, HVA intelligence officers received packages or mailings from them, had telephonic contact with them, and met them outside the United States.

In the Operation “Jack” communications, numerous religious references were used, including referring to Clark as a “brother,” referring to an accommodation address as “Sister Margarete,” and making various coded references to “mass,” “pilgrimage,” “Holy Father,” “Holy Church,” “Holy Relics,” the “Voice of God,” the “Sign of God,” and “missionary work.”

HVA intelligence officers used typical espionage tradecraft to protect the security of their operations. This included, for example, the use of routine shopping excursions as a cover for covert telephone calls and to detect FBI surveillance, limitations on the length of telephone calls, and the use of public telephones to make contact.

As part of his “operational plan” devised with Ziemer, Clark moved to Washington, DC, and obtained a master’s degree in Russian. For a time, Clark worked for a private company in a position that required him to obtain a security clearance. He later obtained a position with the US Army in its environmental law division, which also required a security clearance. Clark had friends who worked for the State Department, and through them he obtained numerous classified documents that he turned over to the HVA.

Squillacote and Stand also moved to Washington, DC, and she went to law school at the HVA’s suggestion. Squillacote first followed in her father’s footsteps by becoming an attorney for the National Labor Relations Board (NLRB). When she realized that she had taken a career path that was not “in the best direction,” she began trying to “move her professional work more in line with the commitments that she had made.” To that end, Squillacote used her father’s connections to obtain an unprecedented temporary detail from the NLRB to the House Armed Services Committee.

In 1991, Squillacote obtained a permanent job as an attorney in the Department of Defense, eventually becoming the Director of Legislative Affairs in the Office of the Under Secretary of Defense (Acquisition Reform), a position that required a security clearance and provided access to valuable information. During her tenure with the Federal Government, Squillacote applied for numerous government jobs, including positions with the CIA; NSA; US Army, Navy, and Air Force; and the Departments of State, Commerce, Energy, and Treasury. Apparently, it was not until she began working for the Department of Defense that Squillacote gained access to the kind of information sought by her handlers.

By the time Squillacote had secured her DoD position, however, the GDR had collapsed. After the fall of the Berlin Wall, Ziemer began working with the Committee for State Security (KGB), the Soviet Union’s intelligence agency. Ziemer maintained his relationships with Squillacote, Stand, and Clark during this time, and they, too, became involved with the KGB.

Squillacote, Stand, and Clark each traveled overseas to meet with Ziemer during the period after the collapse of the GDR. Ziemer instructed all three to purchase Casio digital diaries with interchangeable memory cards. The three Americans, Ziemer, and their KGB contacts communicated with each other by exchanging memory cards.

In April 1992, Ziemer and another former HVA official were arrested and ultimately convicted for their postunification intelligence activities with the KGB. Squillacote, Stand, and Clark became understandably concerned about their personal safety after Ziemer's arrest. They knew that "Western services" were looking for two men and one woman operating out of Washington, DC, and that the Western services were aware of the codenames they had used. They believed, however, that Ziemer and other former HVA officials would not compromise their identities. When Ziemer was released from prison in September 1992, Squillacote, Stand, and Clark reestablished a system of communication with him, one purpose of which was to keep everyone informed about any threats to their safety.

From the beginning of their involvement with the HVA, Squillacote, Stand, and Clark operated independently of each other and generally were unaware of the others' activities. After Ziemer's arrest in 1992, however, the three began talking in detail about their activities and precautions needed to maintain their security. They began discussing the possibility of future intelligence work, perhaps for Vietnam or Cuba. Squillacote also talked to Clark about her interest in South Africa's Communist Party.

In 1994, Squillacote, as part of her search for "another connection," went to Amsterdam to speak to David Truong, whom she had met in college. Truong, who had been convicted of espionage on behalf of North Vietnam, was intrigued, but took no further action.²

In 1995, Squillacote went to great lengths to obtain a post office box under the name of "Lisa Martin." In June 1995, Squillacote, as Lisa Martin, sent a letter to Ronnie Kasrils, the Deputy Defense Minister of South Africa. Kasrils was a Communist Party official and had received training in East Germany, the Soviet Union, and Cuba. The letter, which took Squillacote months to write, was primarily devoted to Squillacote's explanation for the collapse of socialism that began with the fall of the Berlin Wall and her views on how the

Communist movement should proceed in the future. The letter was an attempt by Squillacote to make a connection with Kasrils, whom Squillacote hoped would "read between the lines."

Stand and Clark were aware of Squillacote's letter, but Clark apparently doubted its effectiveness. In February 1996, Squillacote received a Christmas card from Kasrils addressed to L. Martin. In the card, Kasrils thanked "Lisa" for "the best letter" he had received in 1995. Stand and Squillacote were thrilled they had received the note, and they began to think that perhaps a connection could be made.

In September 1996, Squillacote found another letter from Kasrils in her Lisa Martin post office box. The letter stated that, "you may have the interest and vision to assist in our struggle," and invited Squillacote to a meeting in New York City with a representative of "our special components."

Squillacote and Stand, however, were unaware that, for many years, they had been the subjects of an intense FBI investigation. As part of its investigation, the FBI in January 1996 obtained authorization to conduct clandestine electronic surveillance, which included the monitoring of all conversations in their home, as well as calls made to and from their home and Squillacote's office. Through its investigation, the FBI had learned of Squillacote's letter to Kasrils and their response to the February 1996 note from Kasrils. The Kasrils letter of September 1996 was, in fact, written by the FBI as part of a false flag operation intended to uncover information about the previous espionage activities of Squillacote, Stand, and Clark.

When designing the false flag operation, the FBI's Behavioral Analysis Program (BAP) Team prepared a report "to examine the personality of Squillacote and based on this examination, to provide suggestions that could be used in furthering the objective of this investigation—to obtain evidence regarding the subject's espionage activity." The BAP report was based on information the FBI had learned during its extensive investigation and surveillance of the couple.

The BAP report traced Squillacote's family background, including the suicide of her older sister and her mother's history of depression. The report stated that Squillacote was suffering from depression and listed the antidepressant medications she was taking. The primary focus of the BAP report, however, was Squillacote's emotional makeup and how to tailor the approach to her emotional characteristics.

The report described Squillacote as having "a cluster of personality characteristics often loosely referred to as 'emotional and dramatic.'" It recommended taking advantage of Squillacote's "emotional vulnerability" during her period of grieving over the then-recent end of her affair with Ziemer. It further recommended using an undercover agent "who possesses the same qualities of dedication and professionalism as her last contact," and "structuring the undercover agent's pitch" to mirror her relationship with Ziemer. The BAP report also made very specific recommendations about how the false flag operation should be designed:

The following scenario has been developed upon an analysis of the subject's personality, and includes suggestions designed to exploit her narcissistic and histrionic characteristics. It is believed that [Squillacote] will be susceptible to an approach through her mail drop based on her recent rejection by her long-term German handler, and her thrill at receiving a Christmas card from the South African official.

The report suggested the use of a letter from "the object of [Squillacote's] adulation in South Africa." It recommended that the letter instruct Squillacote to travel a circuitous route to the location of the first meeting to "add a sense of excitement and intrigue to the scenario." The report recommended the use of a mature male undercover agent, who should "capitalize on [Squillacote's] fantasies and intrigue" by making a "friendly overture," and "act [ing] professional and somewhat aloof yet responsive to her moods. The initial meet should be brief and leave [Squillacote] beguiled and craving more attention."

The false flag letter received by Squillacote in September 1996 served its intended purpose. Unaware of any FBI involvement, Squillacote and Stand were thrilled about the letter, and Squillacote began enthusiastically making plans for a trip to New York City to meet the South African emissary.

In October 1996, Squillacote met with an undercover FBI agent posing as a South African intelligence officer. She had face-to-face meetings with the agent a total of four times, including one meeting where she brought Stand and her two children. Several letters were also exchanged, including a letter that Squillacote wrote at the request of the undercover agent describing her previous activities with Ziemer. In these meetings and letters, Squillacote expressed her enthusiasm for her new South African connection and her hope for a productive collaboration.

Throughout her association with the undercover agent, Squillacote discussed the possibility of bringing Ziemer and other former East German contacts into the operation. In December 1996, she contacted Ziemer to see if he was interested in the operation. According to Squillacote, Ziemer's response was "[y]es, yes, yes, yes, yes!"

At the second meeting with the undercover agent on 5 January 1997, Squillacote presented the agent with four classified documents she had obtained from the Department of Defense. Although the agent had never requested any documents or classified information from Squillacote, she explained that one day when she and her secretary were alone in her office, she decided to "score what [she] could score." In fact, she had obtained one of the documents even before her first meeting with the undercover agent. The documents Squillacote gave to the undercover agent were:

- *Defense Planning Guidance for Fiscal Year 1997 through 2001*, a numbered document, classified Secret, with restricted dissemination.
- *Defense Planning Guidance Scenario Appendix for 1998 through 2003*, a numbered document classified at the Secret level, which forbade reproduction or further dissemination without authorization.

- *Defense Planning Guidance, Fiscal Years 1996 through 2001, Final For Comment Draft*, which was classified Secret, with restricted dissemination.
- An untitled CIA intelligence report classified Secret, with restricted dissemination.

Three of the documents Squillacote gave to the undercover agent were copies; the *Defense Planning Guidance Scenario Appendix* was an original that Squillacote said would not be missed. These documents formed the basis of the charges against Squillacote and Stand.

Shortly after this meeting, Squillacote quit her job with the Department of Defense; a political maneuver she hoped would put her in position for a more prestigious job.³ Nonetheless, Squillacote continued meeting and corresponding with the undercover agent for several more months until she and Stand were arrested in October 1997.

A search of their home uncovered a wealth of incriminating evidence, including a miniature camera, a Casio digital diary and memory cards, and an extra copy of two of the documents given to the undercover agent. Clark eventually pleaded guilty to a single charge of conspiring to commit espionage, and he testified for the government at the trial of Squillacote and Stand.

At trial, the government introduced certain HVA records, including true name cards showing the names and addresses of Squillacote, Stand, and Clark, as well as documents listing some of their code names and the names of the operations to which they were assigned. The HVA records listed Squillacote as “a developmental agent whose target was the US Government” and described Squillacote as trustworthy.

The records described Stand as reliable and listed him as a source with direct access, with a target of “U.S. union/organization, direct/upper level, IBFG union, U.S.A.” Clark was listed as a “source with direct access,” whose activities were targeted against the “Defense Ministry NATO Country FRG USA.” The records also described Clark as reliable. Other than the four documents passed to the undercover agent, the

government presented no evidence establishing that Squillacote or Stand had previously supplied classified documents or information to Ziemer or anyone else.

Clark pleaded guilty on 3 June 1998 to conspiracy to commit espionage, admitting that he passed classified documents to the former GDR and sought to spy for Moscow as well. On 5 December 1998, Clark was sentenced to 12 years and seven months in prison. Clark had admitted earlier in a plea bargain with prosecutors that he conspired with his two leftist college friends to spy on the United States.

Squillacote and her husband, Stand, were convicted on 23 October 1998, of conspiring to commit espionage, attempting espionage, and illegally obtaining national defense documents. Accused of spying for the former GDR, the former Soviet Union, and South Africa, the couple was described as “Communists on an expense account” who took lavish trips abroad, courtesy of the East German Government, at a time when they had applied for food stamps and for help paying their electric bills. The two also sought jobs in and around the government and stole and smuggled classified documents. Prosecutors never established in court how much the couple was paid for their activities.

On 22 January 1999, Squillacote and Stand were sentenced to lengthy prison terms. A federal judge handed Squillacote a sentence of 21 years and 10 months in prison. Stand received 17 years and six months in prison. The couple had faced a maximum sentence of life in prison for spying. Federal prosecutors argued that the couple should have received longer prison terms, more than 27 years for Squillacote and more than 21 years for Stand, for betraying their country. But the couple’s attorneys sought leniency. The amount of prison time that the judge gave the couple was the minimum required under federal sentencing guidelines.

Squillacote and Stand appealed, raising numerous issues that arose during the course of the prosecution. They filed several pretrial motions to suppress various portions of the government’s evidence. The District Court denied each of the motions, and they challenged those rulings on appeal.

One of their motions, prior to their trial, sought to suppress the evidence of the Foreign Intelligence Surveillance Act (FISA)⁴ surveillance. They attacked the validity of the surveillance⁵ on several grounds, all of which were rejected by the District Court. On appeal, however, they pressed only one FISA-related issue. They asserted that the surveillance was improper because there was no probable cause to believe that Squillacote or Stand were agents of a foreign power. The court disagreed, stating that under FISA, an agent of a foreign power is any person who “knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States.” The court added that a person who knowingly aids and abets another engaging in such clandestine intelligence activities, or one who knowingly conspires with another to engage in the clandestine intelligence activities is also considered an agent of a foreign power.

Squillacote and Stand also sought to suppress the evidence obtained during the search of their home, including the miniature camera, the digital diary and memory cards, a doll with a roll of miniature film hidden inside, and copies of two of the documents Squillacote passed to the undercover agent. They contended that the search was conducted in flagrant disregard of the express terms of the warrant and that the District Court, therefore, erred in denying their suppression motion.

The warrant authorizing the search of their home stated that the government was to search the residence on or before 13 October 1997 (not to exceed ten days)—including serving the warrant and making the search in the daytime between 6:00 A.M. and 10:00 P.M. The search extended over six days, with two FBI agents remaining at the house each night. It was the presence of the FBI agents in the home after 10:00 p.m. that formed the basis of their suppression arguments.

The couple first argued that, by remaining inside their home overnight for five consecutive nights, the FBI searched the home at night, thus flagrantly disregarding the warrant’s time restriction. The

court was not persuaded by this argument. Preliminarily, the court rejected the main premise of their challenge to the search: that the presence of the agents in the house, in and of itself, constitutes a search that should be considered separate and distinct from the authorized search of the residence.

The court concluded that the government did not exceed the scope of the warrant, and even if the government did exceed the scope of the warrant, blanket suppression of all evidence seized would not be required. When denying their motion to suppress, the District Court found that the government complied with the warrant by conducting the search “during the hours that were set out in the warrant.” This conclusion was supported by the affidavit of Special Agent Gregory Leylegian, an FBI agent who took part in the search. Leylegian’s affidavit stated that the FBI “conducted no searching of the premises after 10:00 p.m. each day” and that “the FBI maintained two agents on the premises each night to preserve the integrity of the search process, to expedite the completion of the search, and to maintain security of the premises to prevent the removal or destruction of evidence.”

During the FISA-authorized surveillance, the government intercepted several telephone calls between Squillacote and her psychotherapists. Only the first two of these conversations, however, were listened to or transcribed by the government.⁶ Once the supervising FBI agent learned of the conversations, she instructed the agent responsible for transcribing and indexing the conversations not to listen to, index, or transcribe any other conversations between Squillacote and her therapists.

The couple moved to suppress any evidence derived from the privileged communications and requested a hearing to require the government to prove that the evidence it would present at trial was derived from sources independent of the privileged communications. The District Court refused to hold the hearing, concluding that such a hearing was required only when a constitutionally based privilege was at issue.

On appeal, the couple contended that the FBI employee who listened to and transcribed the conversations between Squillacote and her therapists was involved in the preparation of Squillacote's BAP report and that privileged information was, therefore, used to formulate the false flag operation that led to their arrest. The couple contended that any evidence derived from the privileged information should have been suppressed and that they were entitled to a hearing to vindicate the principles set forth by the Supreme Court in *Kastigar v. United States*, 406 U.S. 441 (1972).

The court, however, concluded that the *Kastigar* case simply was not applicable to this case. In *Kastigar*, the issue was whether a witness who asserts his Fifth Amendment privilege against self-incrimination may be compelled to testify "by granting immunity from the use of compelled testimony and evidence derived therefrom ('use and derivative use' immunity), or whether it is necessary to grant immunity from prosecution for offenses to which compelled testimony relates ('transactional' immunity)."

Because this case did not involve the use of compelled testimony, the District Court refused the appellants' request for a *Kastigar*-type hearing. In addition, because the privilege at issue here was not a constitutional one, the District Court refused to suppress any evidence arguably derived from the government's interception of the two conversations with Squillacote's therapists.

Perhaps some of the most damaging evidence introduced against Squillacote and Stand at trial were the HVA documents—the true name cards listing their names and their codenames and the agent data sheets showing the nature of their assignments for the HVA. The couple moved to prevent the introduction of these documents, but the District Court denied the motion. On appeal, they contended that the documents were improperly admitted, arguing that they were not properly authenticated and that, even if authenticated, the documents were inadmissible hearsay. The Federal Rules of Civil Procedure provide that official records of a foreign country

are considered properly authenticated if the records are attested by a person authorized to make the attestation, and accompanied by a final certification as to the genuineness of the signature and official position (i) of the attesting person, or (ii) of any foreign official whose certificate of genuineness of signature and official position relates to the attestation or is a chain of certificates of genuineness of signature and official position relating to the attestation.

In this case, the government presented a certification from Dirk Dorrenberg, the director of the counterespionage and protective security department of the *Bundesamt für Verfassungsschutz*, the counterintelligence service for the unified Federal Republic of Germany (FRG). In his certification, Dorrenberg stated that the FRG is the legal successor to the GDR and that he had the "authority to make this certification by virtue of [his] official position and area of expertise."

Dorrenberg stated that he had compared the HVA documents introduced by the government to "actual duplicates" of the original records, and he certified that the government's copies were "true and correct copies" of "genuine and authentic records" of the HVA. Dorrenberg also certified that the signature of Lothar Ziemer appearing on some of the records was "genuine and authentic."

The government also presented a final certification from Manfred Bless, an FRG representative "assigned and accredited to the United States as a Counselor, Political Section, of the Embassy of the Federal Republic of Germany, in Washington, D.C." In this final certification, Bless certified that Dorrenberg held the position claimed in the Dorrenberg certification and that Dorrenberg was authorized to make the certification. These certifications comply in all respects with the requirements of Rule 44(a)(2) and Rule 902(3). Therefore, whether the documents are considered official documents or official records, the District Court concluded that the government adequately authenticated the HVA documents.

The couple, however, contended that the certification process of Rule 902(3) is intended to confirm the signature or attestation contained in the offered document. According to them, if the document being offered into evidence does not contain a signature, then a self-serving declaration of authenticity is meaningless. Thus, they contended that many of the HVA documents were not subject to self-authentication under the rules because the documents themselves were not signed or did not contain an attestation.

The court ruled that this argument is without merit. Nothing in Rule 44(a)(2) or in Rule 902(3) requires that the documents themselves be signed or contain an attestation within the body of the document. The rules are written in the alternative—foreign documents may be authenticated by a certification from the official executing the document or by an official attesting to the document. Thus, so long as a proper official attests that the proffered document is true and genuine, it simply does not matter whether the document itself is signed or contains its own attestation.

As noted above, Rule 44(a)(2) also requires a final certification regarding the signature and position “(i) of the attesting person, or (ii) of any foreign official whose certificate of genuineness of signature and official position relates to the attestation or is in a chain of certificates of genuineness of signature and official position relating to the attestation.” Seizing on these requirements, the couple contended that neither the Dorrenberg certification nor the Bless certification establish that “Dorrenberg is an official ‘whose certificate of genuineness of signature and official position relates to the execution or attestation’ or that his certificate is in a ‘chain of certificates of genuineness of signature and official position relating to the execution or attestation.’ ”

The court ruled that this second argument was likewise without merit, as it was premised upon a fundamental misapprehension of the requirements for the authentication of foreign documents. An examination of Rule 44(a)(2) and Rule 902(3) reveals two requirements for the authentication

of a foreign document. First, there must be some indication that the document is what it purports to be. Thus, a proper official in his official capacity must execute the proffered document, or a proper official must attest to the genuineness of the document in his official capacity.

In this case, the government satisfied the first requirement of establishing that the HVA records were what they purported to be by presenting Dorrenberg’s certification that the government’s records were true and accurate copies of genuine HVA records. The government then established that the official vouching for the document was who he purported to be in the first manner described above—by presenting a final certification from another official establishing that it was Dorrenberg’s signature on the proffered certification and that Dorrenberg was authorized to attest to the authenticity of the HVA documents.

Because the government established the genuineness of the signature and position of the person attesting to the documents, the portions of the rules dealing with officials that related to the execution or attestation in the chain of certifications were not applicable. Finally, contrary to the couple’s suggestions, the rules do not require the official attesting to the genuineness of foreign documents or records to have possession or custody of the proffered documents, to be an expert in handwriting analysis, or to have been associated with the foreign government at the time the documents were created.

The couple also challenged the District Court’s ruling that the HVA documents were admissible as statements of a coconspirator under Rule 801(d)(2)(E) of the Federal Rules of Evidence. The Appeals Court reviewed the District Court’s admission of evidence under Rule 801(d)(2)(E) for an abuse of discretion. In the Appeals Court’s view, the District Court properly admitted the HVA records as statements by a coconspirator.

First, the indictment specifically charged the couple with conspiring with, among others, “agents and officers of the GDR,” and the

government presented ample evidence supporting that allegation, including the government's overwhelming evidence of their relationship with Lothar Ziemer, whose signature appears on many of the disputed HVA documents. Second, although some of the documents are undated, many bear dates within the text that are clearly within the course of the conspiracy as defined by the government's evidence. Many of the undated HVA documents show the same registration number as the dated documents and the documents bearing Ziemer's signature, thus establishing a connection between all of the HVA documents. Accordingly, the government's evidence demonstrated that the statements were made during the course of the conspiracy. Third, there can be no real dispute that, by compiling the information contained in the disputed documents—the couple's real and code names, their addresses, the object of their assignments, and how they could be contacted—the GDR was acting in furtherance of the conspiracy.

Although the identity of the declarant of the unsigned documents may not be known, the only conclusion that can be drawn from the information included in the documents—information that was corroborated in many respects by Clark's testimony and by Squillacote's own statements to the undercover agent—is that the documents were created by or at the direction of East German agents who had knowledge of and were involved in the conspiracy with them. While there may be cases where the inability to identify the declarant of an alleged coconspirator's statement could render the statement inadmissible, this is not one of those cases. The HVA documents were sufficiently connected to each other and to the conspiracy established by the government's evidence to make them reliable and admissible under Rule 801(d)(2)(E), notwithstanding the government's inability to identify the declarants. The Appeals Court, therefore, concluded that the HVA records were properly authenticated and were properly admitted as statements of coconspirators.

Finally, the couple raised numerous issues in connection with the District Court's instructions to the jury. Their challenges involved the District

Court's instructions on their entrapment defense, the court's failure to include an instruction on multiple conspiracies, and its explanation to the jury of "information relating to the national defense."

Squillacote and Stand contended that the government's first contact with Squillacote—the phony Kasrils letter—was an "approach," not an "encounter," because encounter can mean only a face-to-face meeting. Thus, they argued that, by instructing the jury to consider predisposition that existed before the first encounter with the government, the jury may have concluded that Squillacote became predisposed to commit the crimes only after receiving the Kasrils letter, but still rejected the entrapment defense because the disposition arose before Squillacote met the undercover agent for the first time. The Appeals Court believed that the District Court's instruction sufficiently directed the jury's focus to the proper time frame for determining the existence of Squillacote's predisposition, particularly since there was no dispute that the government's first contact was the Kasrils letter.

Squillacote clearly was in the position to commit the crimes with which she was charged. After years of trying, Squillacote finally had a job that provided her with access to classified information and documents. She had received excellent training in the arts of espionage, and she had a long relationship with a "spy-master" who was trying to find another connection interested in the services that she and her coconspirators could provide. In addition, as evidenced by her approach to David Truong—the convicted spy—and her letter to her South African hero, Squillacote herself was actively searching for another customer for her skills. Thus, Squillacote was in the position to become an active spy even without the help of the undercover agent. If the evidence in this case did not establish Squillacote's readiness, then the Appeals Court could not imagine what would be sufficient to do so.

The couple's theory of the case was that the FBI, through its BAP report profiling Squillacote, masterfully catalogued Squillacote's every emotional and psychological vulnerability. The

FBI then used this information to devise an undercover operation exploiting these weaknesses to ensure that Squillacote would fall for the undercover agent's pitch. The couple claimed that the agent induced Squillacote into going along with his scheme by making subtle psychological appeals to which he knew Squillacote would be uniquely vulnerable. Consistent with this theory of entrapment, the couple's lawyer requested the following instruction on entrapment:

Entrapment occurs . . . [w]here the Government goes beyond providing an opportunity for a crime but instead induces its commission by taking advantage of the defendant through such persuasion as appealing to the defendant's political beliefs or to some other alternative, non-criminal type of motive, or by playing on defendant's personal sympathies and life experiences, or by exploiting the unique vulnerabilities of the defendant. The law of entrapment forbids the conviction of [a] person where the Government has played on the weaknesses of an innocent party and beguiled her into committing crimes which she otherwise would not have attempted had the Government not induced her.

The District Court refused to give this instruction. Instead, the court instructed the jury as follows:

A person is entrapped when that person has no previous disposition or willingness or intent to commit the crime charged and is induced by law enforcement officers to commit the offense. In determining the question of entrapment, you should consider all of the evidence received in this case concerning the intentions and disposition of the defendant before encountering the law enforcement officer, as well as the nature and the degree of the inducement provided by the law enforcement officer.

In the Appeals Court's view, the evidence of Squillacote's predisposition can only be described as overwhelming. The government's evidence established that Squillacote's involvement with the HVA went back almost twenty years. Through her

East German contacts, Squillacote learned how to determine if she was being followed and how to evade those who might be following her, how to receive and decipher sophisticated coded messages, how to use the miniature document camera, and how best to remove any "classified" markings on documents. After the fall of East Germany, when Squillacote finally had a job that gave her access to sensitive information, Squillacote herself sought out opportunities to use these skills. She contacted David Truong, a convicted spy, in the hopes of establishing a new "connection," and she sent her fan letter to Kasrils, the South African official, hoping that he would "read between the lines." That Squillacote actively sought employment as a spy is powerful evidence that she was disposed to committing espionage well before the government first contacted her.

Squillacote's response to the government's phony Kasrils letter was also strong evidence of her predisposition. It was perhaps an understatement to say that Squillacote was ecstatic when the Kasrils letter arrived in the mail. When she received the letter, Squillacote called her brother to tell him about the letter. While laughing and crying, Squillacote said, "Michael, I did it. I did it Mike. All those years. All those years and I did it. I did it."

To her husband, Squillacote described the letter as "really, really, really, amazing." In fact, Squillacote was so excited when she received the phony letter that she even told her children about the impending meeting. In another telephone conversation with her brother, Squillacote explained how proud she was that Kasrils had "read between the lines" of her letter. Squillacote's predisposition to commit espionage is also evidenced by her statements to the undercover agent during their first meeting.

In that meeting, the agent identified himself as being with the South African Intelligence Service, and he explained that, "there are still operations being conducted without the full knowledge of everybody in the state, for reasons, I guess, you can well understand." Squillacote responded that "[t]his is an area that's not unfamiliar to me."

Squillacote then elaborated that she had been associated with similar activities “in another kind of capacity” for many years, “so, you should understand that this is not a tabula rasa for me. I’m coming with a history.” Squillacote described her covert activities as her “raison d’être.” When the undercover agent told Squillacote that he had “done some things that this government would consider to be illegal,” Squillacote responded, “[b]een there,” and she explained that she had “violated Federal eighteen, lots and lots.”⁷

To the Appeals Court, these statements clearly showed that Squillacote was more than willing, without any encouragement from the government, to commit espionage. Perhaps the most compelling evidence of Squillacote’s predisposition is related to the documents she passed to the undercover agent at their second meeting.

The government’s evidence established that Squillacote obtained one of the documents sometime before her first meeting with the undercover agent, even though the phony Kasrils letter did not request, or even suggest, that Squillacote bring any classified materials to the meeting. Extra copies of two of the documents were found in Squillacote’s home when the government executed its search warrant. Thus, even before she first met the undercover agent, Squillacote had already violated 18 U.S.C.A. § 793(b) by taking or copying classified national defense information. Clearer evidence of predisposition is difficult to imagine.

The government’s evidence established that Squillacote, Stand, and Clark were involved in a single conspiracy to compromise information related to this country’s national defense. Stand, who was recruited by Ziemer, recruited both Clark and Squillacote. Ziemer was the primary handler for Stand, Squillacote, and Clark, and the three received largely the same training and used the same methods of communicating with their East German contacts. After the collapse of the GDR, the three continued their relationships with Ziemer, which expanded to include the KGB. With the knowledge of the other conspirators, Squillacote also sought to develop new contacts with others who might be interested in what the group had to offer.

Stand was aware of Squillacote’s letter to Kasrils, as well as her meetings with the undercover agent. In fact, Stand helped Squillacote remove the classified markings from the documents she provided to the agent. Clark was likewise aware of the letter she wrote to Kasrils, and Squillacote sought to involve Stand, Clark, and Ziemer in the operation after the undercover agent contacted her.

In the Appeals Court’s view, this evidence was more than sufficient to support the finding of a single conspiracy. That Squillacote, Stand, and Clark were not always aware of the others’ activities is part of the standard operating procedure for those engaged in espionage and would not prevent the jury from determining that a single conspiracy existed.

Although it is possible that Squillacote’s South African foray could be viewed as separate from the original conspiracy, it was certainly closely related to the conspiracy charged in the indictment, a conspiracy in which the evidence overwhelmingly established the involvement of Squillacote and Stand. Therefore, because the evidence did not establish that the couple was involved “only in ‘separate conspiracies unrelated to the overall conspiracy charged in the indictment,’ ” the District Court properly refused to instruct the jury on multiple conspiracies.

The couple made much of Clark’s testimony on cross-examination that he did not have an agreement with them to commit espionage, that he lost contact with them for several years in the late 1970s and early 1980s, and that he was not involved in the South African effort. Given that Clark pleaded guilty to the charge that he conspired with Squillacote and Stand to commit espionage, it seems unlikely that the jury would have found this testimony particularly persuasive. In any event, to accept this argument would have required the Appeals Court to consider only Clark’s testimony and to ignore the other evidence tending to show the existence of a single conspiracy or multiple—but still related—conspiracies, which, of course, the Appeals Court did not do at this stage of the proceedings.

After carefully reviewing the record and considering the arguments of the parties, the Appeals Court found no reversible error in the proceedings. Accordingly, the convictions of Squillacote and Stand were affirmed.

In April 2001, the Supreme Court declined to hear an appeal by Squillacote and Stand, which challenged the government's ability to obtain wiretaps and search warrants under FISA on the basis of secret evidence. Attorneys for Squillacote and Stand argued that prosecutors should have been forced to show them the evidence underlying a FISA wiretap that remained on a telephone at the couple's home for 550 days.

Endnotes

¹ *Ministerium fur Staatssicherheit*.

² David Truong, also known as Truong Dinh Hung, and Ronald Louis Humphrey were sentenced on 7 July 1978 to 15 years each in prison for espionage. Humphrey, a US Information Agency officer, met Truong while trying to get his mistress and her children out of Vietnam in the mid-1970s. Truong, who portrayed himself as an anti-Communist, had many official contacts in the US Government, including contact with William Colby at the CIA. The FBI arrested the two men on 31 January 1978 and charged them with seven counts of espionage on behalf of North Vietnam. Humphrey took classified State Department documents and passed them to Truong who handed them over to a courier for delivery to North Vietnamese officials.

³ However, Squillacote explained to the undercover agent that her involvement in the political maneuvering and her decision to quit were primarily motivated by her "joint efforts" with the undercover agent. Squillacote believed that her former Department of Defense boss might be named Deputy Secretary of Defense and that she would be able to follow her former employer back into the Department. Squillacote described this scenario as "the big time," noting that if it worked out, there would be a "straight f---ing line," presumably to the Secretary of Defense. This scenario never came to pass.

⁴ FISA was enacted "to put to rest a troubling constitutional issue" regarding the President's "inherent power to conduct warrantless electronic surveillance in order to gather foreign intelligence in the interests of national security," a question that had not been definitively answered by the Supreme Court. FISA thus created a secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this nation's commitment to privacy and individual rights.

⁵ The government conducted 550 consecutive days of clandestine surveillance of them, surveillance that was authorized under the Foreign Intelligence Surveillance Act of 1978.

⁶ Actually, one of these conversations was between Stand and one of Squillacote's therapists. Because Squillacote gave the therapist permission to talk to Stand, the court assumed for purposes of their motion that the conversation was privileged, and, in the interest of convenience, the court referred to both conversations as having taken place between Squillacote and her therapists.

⁷ Given the context, it is apparent that this statement is a reference to Title 18 of the United States Code, which is entitled "Crimes and Criminal Procedure."

French SIGINT Targeting

The French magazine *Le Point* reported in June 1998¹ that France systematically listens in on the telephone conversations and cable traffic of many businesses based in the United States and other nations. The article also reports that the French Government uses a network of listening stations to eavesdrop and pass on commercial secrets to French businesses competing in the global economy.

The article goes on to state that the French secret service, DGSE, has established listening posts in the Dordogne (southern France) and also in its overseas territories, including French Guiana and New Caledonia. The article attributes to an unnamed “senior official within this branch of the French secret service” the claim, “This is the game of the secret war,” adding that US listening posts do the same. The magazine report says that Germans who bought into the French Helios 1A spy satellite system are being given access to political and economic secrets as part of a Franco-German agreement to compete with a commercial information agreement between the United States and Britain.

According to multiple sources, on 5 July 1999, TotalFina—the Franco-Belgium oil company—initiated a \$43 billion hostile takeover bid to buy the French oil company Elf Aquitaine. Elf formally rejected the takeover bid and on 19 July offered a counterbid of \$51 billion. After two months of acrimony, the takeover battle ended when both companies announced they had agreed to a friendly merger. The TotalFina–Elf merger would result in the world’s fourth-largest oil company, ahead of Chevron and Texaco, but still well behind Exxon-Mobil, Royal Dutch Shell, and BP-Amoco-Arco.

The struggle of these two world-class companies is characteristic of the hostile takeover era that has dawned in Europe. According to Mr. Terry Desmarest, President and Chief Executive of TotalFina, the grab for Elf was “to assure continued solid growth and to take our place as an oil major of the first rank, at a time when the industry is restructuring on a global basis.”

But wait; could there be more to this story than meets the eye? Did TotalFina beat Elf to the punch? Perhaps it did, but according to Paris *Le Monde*, which cited London’s *Financial News*, TotalFina’s bid followed an indiscretion on the part of two of Elf’s advisory bankers discussing preparations for a raid on TotalFina that prompted Desmarest to carry out his surprise attack. The indiscretion took the form of a conversation between the two French bankers on a flight between London and Paris. Unfortunately for Elf, the conversation was overheard by a TotalFina financier traveling on the same flight who chose to disregard the old adage that a gentleman does not eavesdrop on other people’s conversations.

The French article goes on to discuss the gravity of the situation, noting that, according to one source, “travelling constantly, business bankers, who spend days and nights preparing a takeover bid, sometimes commit indiscretions due to tiredness. Shouting on a mobile phone in a business class waiting room, reading presentation documents during a flight, or boasting to a colleague are all high risk actions.” The article further notes, “the new boys are easily recognizable in the plane. They get out their files as thick as a telephone book, whereas the veterans have a nap or read a bestseller.”

According to the *Sunday Times*² (London), French intelligence is intercepting British businessmen’s calls after investing millions of francs in satellite technology for its listening stations. Since the French Government upgraded its signals intelligence capabilities last year, secret service elements are now using it to tap into commercial secrets. At least eight centers scattered across France are being “aimed” at British defense firms, petroleum companies, and other commercial targets.

Eavesdroppers can “pluck” digital mobile phone signals from the air by targeting individual numbers or sweeping sets of numbers. Targets have included executives at British Aerospace (BAe), British Petroleum, and British Airways, according to French sources.

Senior executives have been told not to discuss sensitive issues on mobile phones, and BAe staff have been told to be “especially careful” during campaigns for new business, such as the current battle to supply Eurofighter missiles.

An executive within one British defense firm said, “Top people use the same mobile telephones as anyone else, without any sort of high-tech security equipment. There is an understanding that we need to be careful. People never say anything that they would not want heard elsewhere —especially at sensitive times and during projects when other people may have an interest in listening.”

A source in Paris with links to French intelligence said: “It is not fair to say that France is constantly listening to British or German companies, but there may be times when certain areas might be targeted.”

This report comes on the heels of another *Sunday Times* article in late 1999, which reported that BAe executives were burglarized at a Toulouse hotel by French secret service agents involved in industrial espionage. The raid is believed to have been carried out by a *Direction et Surveillance du Territoire* (DST) unit called *Protection du Patrimoine Economique*, which is said to conduct specialized break-in operations targeting foreign companies.

The agents allegedly searched briefcases and stole documents from BAe officials while they were meeting with officials from the French aviation company, Airbus Industrie. The French officials, who apologized and returned photocopies of the company documents, notified the British. The incident involved at least four BAe staff members who were discussing aviation contacts and BAe’s future relationship with Airbus.

Endnotes

¹ See *Le Point*, 6 June 1998, pp. 61-64.

² See *Sunday Times*, 23 January 2000.

Updates on Two Espionage Cases

(Editor's Note: Information on the espionage cases of Douglas F. Groat and Robert Kim appear in Volume III of the CI Reader on pages 408 and 341, respectively. Since then the following activities have occurred in their cases.)

Douglas F. Groat

On 25 September 1998, former CIA covert operative Douglas F. Groat was sentenced to five years in prison after having pleaded guilty in July to one count of extortion. He had attempted to extort \$1 million from the Agency in exchange for his silence about overseas operations. As part of the plea agreement, Federal prosecutors dropped four counts of espionage.

According to the indictment, Groat not only disclosed damaging intelligence information to foreign countries, but also tried to extort more than \$500,000 from the CIA under the threat he would tell certain governments of highly classified CIA operations. Prosecutors refused to identify the two countries Groat allegedly aided.



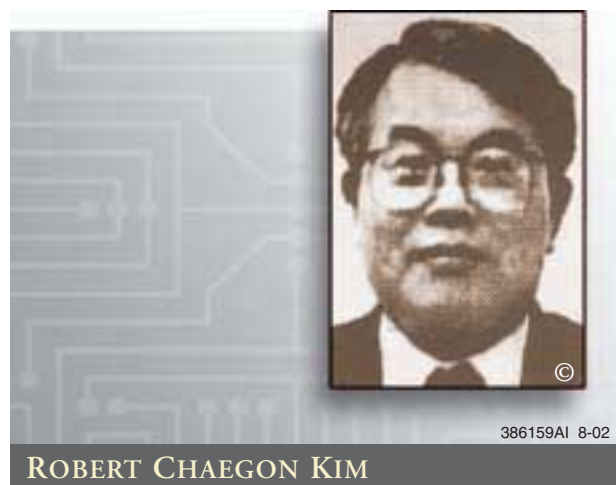
The CIA employed Groat from 1980 to 1996, where he worked in the Science and Technology Directorate. In the spring of 1993, he was placed on administrative leave for "personnel" issues and was fired three years later. Intelligence officials, and Groat's own relatives, have described him as a

disgruntled employee who was under suspension for botching an overseas operation involving a break-in at a foreign embassy.

The plea agreement eased prosecutors' concerns that a trial on all the charges might have forced them to disclose sensitive information in open court. On the other hand, the initial charges could have carried the death penalty. Groat agreed to help the government sort out whether his activities during or after his tenure at the Agency breached national security, and he agreed to submit any books, articles, or interviews to federal officials for security review.

Robert Kim

On 4 October 1999, the US Supreme Court rejected, without comment or dissent, an appeal by Robert Kim, 59, who is serving a nine-year sentence for spying on behalf of South Korea. Kim, a former US Navy computer technician who was arrested in 1996, argued that his civil rights had been violated and that his status as a naturalized US citizen, rather than a US citizen by birth, added to the severity of his sentence. He admitted shortly after his arrest that he had collected military documents to pass on to a captain in the South Korean Navy. The US Justice Department had asked the Supreme Court to reject Kim's appeal.



A South Korean Foreign Affairs and Trade Ministry spokesman said that his government would not get involved in the case, noting that "the government

is not in a position to officially get involved in a US Court's ruling on Kim's espionage conviction, which went thorough US legal procedures."

The "Committee To Rescue Robert Kim," which was originally established in March 1997 but remained dormant until 1998, held an emergency meeting at Seoul's Koreana Hotel on 31 October 1998 to start a campaign to rescue Kim. The committee, composed of some 100 people, decided to set out on a full-scale campaign because of their disappointment in former President Kim Yong-sam who visited the United States in 1998 and said "the ROK Government would not interfere in the matter because Robert Kim is an American." Headed by Ryu Chae-kol, vice president of the National Congress for New Politics (NCNP), Yi T'ae-pyon, a member of the United Liberal Democrats (ULD) and lawyer Yi Se-chung, the committee planned to urge President Kim Tae-chung to make diplomatic efforts to have Kim released. They also decided to send a written petition with the joint signatures of members of the National Assembly to the US Government. In addition, the committee planned to stimulate public interest using personal computers and to launch a signature campaign together with social and human rights groups.

Yi said the committee would stage a rally calling for the release of Robert Kim in front of the US Embassy on 20 November 1998, during President Clinton's visit to the Republic of Korea (ROK). The rally will show the united stance of the South Korean people, albeit somewhat belatedly.

The committee planned to make various efforts to support Kim's family in their daily lives. Since June 2000, Yi Ung-chin, president of the Sonu marriage consultant office and member of the committee, sent 1 million won monthly to Kim's elderly mother (77) and his wife (53). Since her husband was put in prison, Robert Kim's wife has been working as a janitor in churches.

According to South Korean media reporting, Kim is proud of what he did and showed his patriotism

in prison. With regard to his espionage charges, Kim stated, "I am not a spy from the ROK, and likewise I am not a hero. While dealing with much intelligence, I decided to dedicate my life to improving the weakness of my country, a minority, because I knew what intelligence our country needed politically and technologically."¹

In an appeal at the National Assembly on 14 November 1998, Representative Kim Sung-gon, brother of Robert Kim and a member of the National Congress for New Politics, urged the government to push for US acceptance of the re-sentencing demand when Kim talks with Clinton. Representative Kim, as an opposition leader, wrote a petition to the US Government calling for his brother's release. But as President of the National Assembly, he opposed an Assembly resolution on the issue, saying that the decision of the U.S. court must be respected.

He said, legally, his brother is guilty, but the sentence imposed was too severe because his brother was not exactly "spying." Kim is seeking his brother's release from a humanitarian standpoint. "What he engaged in was just delivery of classified documents, not spying," said Representative Kim. "He didn't get any money from our government and he's not employed by our government." Kim feels that the passage of secret information between countries with friendly relations with a wide gap in information acquisition capabilities is only natural. "The imbalance between the United States and South Korea in terms of intelligence will cause these kinds of things (leaking of secrets) to happen," said Representative Kim.

According to Kim, South Korea is virtually dependent on the United States for vital information on national security and North Korea. He argued that his brother's passage of "routine" documents was a great help to Korea, but no great loss for the United States. He added that his brother, while being a US citizen, is still a Korean at heart. It seems he was compelled by patriotism to hand the material over to the Colonel Baek Dong-il, the embassy attaché he met through his supervisor.

Representative Kim believes in his brother's innocence but did not have any illusions about his brother's situation. "The chance is not very high (that he will be released), but still I believe that if he's innocent, God will help him," he said.²

Endnotes

¹ *Seoul Chungang Ilbo*, 2 November 1998.

² *Korean Herald*, 21 November 1998.

Cuban Spies in Miami

In 1995, after obtaining FISA (Foreign Intelligence Surveillance Act) Court approval, the FBI obtained warrants to surreptitiously search apartments and monitor telephone communications by a group of Cubans who were Cuban intelligence operatives. The group, through its principal agents or illegal officers, communicated directly with the Cuban Government about its activities and received specific missions and taskings from the Cuban Government. The instructions were subsequently relayed to the other members of the spy ring as appropriate.

During the searches, the FBI uncovered and read the contents of the communications from and to the Cuban Government. This information was concealed in hidden files on computer floppy diskettes kept in the residences of three of the principal agents.

At Cuban Government direction, the Cuban spy ring collected and reported information on domestic, political, and humanitarian activity of anti-Castro organizations in the Miami-Dade county area; the operation of US military installations; and other US Government functions, including law enforcement activity. The spy ring also carried out tasks in the United States as directed by the Cuban Government, which included attempted penetration of US military installations, duplicitous participation in and manipulation of anti-Castro organizations, and attempted manipulation of US political institutions and government entities through disinformation and pretended cooperation. The spy ring received financial support from the Cuban Government to carry out its tasks.

An analysis of the communications used by the spy ring revealed that they spoke and addressed each other and their agents as representing the Cuban Government. They referenced decision-making "by the High Command," referred to individuals as "comrade," and used names and abbreviations associated with Cuban Government organizations. Communications between the

members also referenced the “Intelligence Information Department”; “C.P.” for *centro principal* or headquarters; “MINIT” for Ministry of Interior—which administers the Cuban Directorate of Intelligence or DI; and “DAAFAR,” a known abbreviation for the Cuban Air Force Command. They also used jargon and abbreviations such as “S.E.E.” (*Servicios Especiales Enemigos*) that refers to the FBI or CIA.

The spy ring members paid great attention to maintaining secrecy as to their identity and mission and took elaborate steps to evade detection. They called themselves “*La Red Avispa*”—The Wasp Network. They used code names, including “Giro,” “Castor,” “Lorient,” “Vicky,” “Franklyn,” “Allan,” “Manolo,” “Judith,” “Mario,” and “Julia.” They spy ring also used false identities, including assuming the name, date of birth, and social security number of a deceased person. The ring is viewed as the largest Cuban espionage operation uncovered in the United States in a decade.

On the basis of its investigation and surveillance, the FBI had identified three individuals as the spy ringleaders by 1998. The first was Gerardo Hernandez who had oversight for infiltrating his subagents into US anti-Castro groups in the Miami area. The second leader was Ramon Labanino whose primary task was to penetrate and report on US military installations and activity in the South Florida area, including the Southern Command and the Boca Chica Naval Air Base in Key West. The third leader was Fernando Gonzalez, who took over Labanino’s responsibilities, including meeting with subagents when Labanino was tasked with Cuban Government missions outside the Miami area.

Hernandez and Labanino received reports from, and provided payments to, their respective subagents and tasked their subagents based on instructions they received from Cuba. Ricardo Villareal and Remijio Luna also exercised managerial or supervisory functions over subagents at times, but both men left the United States for other operational assignments.

Geraldo Hernandez

Geraldo Hernandez, who was known as Manuel Viramontes in Florida, used the code names “Giro” and “Giraldo.” He resided at 18100 Atlantic Boulevard, Apartment 305, North Miami Beach. He was arrested there in the early morning hours of 12 September 1998. He had been in the United States since 1992. The FBI bugged his apartment, picking up numerous conversations by Hernandez regarding his Cuban intelligence activities. The press identified him as a captain in Cuban intelligence.¹

An FBI search of the apartment revealed a shortwave radio, computers, numerous 3.5 floppy diskettes, recording devices, and photographic equipment. Hidden on the floppy diskettes were literally thousands of pages of lengthy, detailed narrative reports between Hernandez and the Cuban Government, as well as between Hernandez and the various subagents in his network—“Castor,” “Franklyn,” “Lorient,” “Judith,” and “Manolo.”

Hernandez’s managerial and supervisory role within the spy ring is reflected in the computer records. They show that he communicated by telephone and met frequently with the other senior agents of the ring, including Labanino, Villareal, and Luna in various combinations and that countersurveillance measures were taken to avoid detection. When using the telephone, Hernandez used coded language and a false Puerto Rican accent.

He had a budget and routinely submitted a financial report detailing expenses for the “operation base” and “management of (the) agent network,” as well as cash payments to various subagents to Cuba. In one communication from Cuba, Hernandez was advised that “(b)ecause of the economic state of our country, headquarters has been obligated to reduce the budget of all the comrades there.”

Hernandez received detailed instructions from Cuba directing him to task individual subagents within the “theater of operations” with specific missions. He ensured that the missions or taskings were accomplished and reported the results to

Cuba. He also frequently offered his analysis and interpretation of events and information in his communications to Cuba.

Among the many communication topics between Hernandez and Cuba or his subagents were:

- The infiltration of the US Southern Command headquarters in Miami—according to Cuba, “one of the new prioritized objectives that we have in the Miami area.”
- The activities of Cuban exile groups in Miami and tactics to disrupt those groups by, among other things, “creat(ing) animosity” between specified groups and attempting to discredit certain individual leaders.
- The activities at the Boca Rica Naval Air Station as well as reports on an apparent military topic identified by Cuba that “continues to be of great importance to our comrades at DAAFAR.”
- The manipulation of the media, political institutions, and public opinion, including using anonymous or misidentified telephone calls and letters to media and political figures.
- Specific security precautions to be undertaken to avoid detection.

Other communications reference false identities used by Hernandez—he stole the identity of a dead man—as well as an “arrest alibi” and an escape plan to flee the United States. He had four escape routes—two via Mexico and one each in Canada and Nicaragua. He also had three different covers prepared, which included personal histories, details of schools and jobs, and names of relatives. He was explicitly directed that, under no circumstances, was he ever to “admit to being part of, or linked to, Cuban intelligence or any other Cuban government organization.”

A frequent topic of the messages within the files is the methods by which the spy ring communicates with each other and particularly their use of computers and floppy diskettes to deliver messages to each other.

Hernandez kept diskettes that appear specifically to have been delivered by, to, or exchanged with “Lorient,” “Castor,” “Franklyn,” “Oso,” and “Horacio.” Precise communications procedures and instructions as to how the computers and diskettes were to be used was often the subject of messages between the ring members. In one such communication, Hernandez references “codes to decrypt operational base diskettes.” He also directly communicated to other senior agents—“Horacio” and “Rami”—about specific problems he was having with his computer.

Among the documents discovered was a sabotage operation—codenamed Operation Picada—which targeted buildings and aircraft in Florida.

Ramon Labanino

Ramon Labanino, who was known as Luis Medino, resided at 1776 Polk Street, Apartment 3G, Hollywood, Florida, and was arrested there in the early morning hours of 12 September 1998. He used the code name Allan. A press article identified him as a major in Cuban intelligence and said he was featured in an FBI videotape exchanging folders in a Wendy’s restroom with a Cuban UN diplomat.² Before his assignment to Miami in 1996, he operated in the Tampa, Florida, area from as early as 1992, reporting information to Cuba regarding operations at McDill Air Force Base.

Electronic surveillance of his apartment reflected numerous conversations up to September 1998 on activities on behalf of the Cuban Government. A search of the apartment revealed a computer, numerous floppy diskettes containing concealed messages dating back to 1992, a shortwave radio, and recording equipment.

Labanino was transferred specifically to lead the effort to infiltrate the US Southern Command. In communications received from Cuba in late 1996, he was advised: “Headquarters decided that the Southern Command, which will soon be stationed in Miami, should be assigned to a group of comrades under the direction of Allan. The Comrades are Mario and Julia, Gabriel and Lorient.”

The computer records seized from Labanino's apartment exposed codes, encryption procedures, and messages regarding the quality of radio message traffic received from "C.P." In his communications, Labanino referred to himself as an "illegal officer." The communications also contained at least one reference to his "comrades from C.P." He also discussed how he obtained a false driver's license in the name of "Luis Medina," his assumed identity.

Labanino had meetings with other principal agents, including "Giro," "Horacio," and "Rami," and used codewords when speaking with them. In addition, computer records showed that Labanino received reports from his subagents about the Southern Command and the Boca Chica Naval Air Station.

Prior to his arrest on 12 September 1998, he had planned to flee the United States on 17 September because his brief case had been stolen while he was in Los Angeles the previous week. The briefcase contained various espionage paraphernalia as well as school diplomas, a birth certificate, \$5,000 in cash, and a video shot in Cuba.³

Antonio Guerrero

Antonio Guerrero, a.k.a. "Lorient," resided at 30161 Poinciana Road, Big Pine Key, Florida, where he was arrested in the early morning hours of 12 September 1998. His girlfriend, with whom he resided, owns the house. He was a civilian employee of the US Navy, Public Works, Boca Chica Naval Air Station, Key West. According to the news media, Guerrero grew up in Cuba and studied engineering in the Soviet Union. He worked menial jobs at Boca Chica Naval Air Station for more than five years.⁴

In the past, Guerrero reported to Hernandez who was tasked by Cuba "if . . . necessary, to go to Key West every two weeks to pick up information (Lorient has) obtained . . ." Surveillance of Guerrero identified him meeting and exchanging bags with Hernandez. Later, Labanino assumed handling of Guerrero. Guerrero reported his activities and received taskings from both Hernandez and Labanino via the exchange of floppy diskettes.

Guerrero was specifically tasked to report any "unusual exercises, maneuvers, and other activity related to combat readiness" at the air station. Guerrero did, in fact, report detailed information regarding the daily activities at the air station, including—through the use of beeper codes—the type of aircraft being deployed there; precise physical descriptions of the interior and exterior of a structure at the air station, which he suspected of being prepared for top secret activity, such as supposed "electronic warfare" aircraft believed to be deployed "to activities of exploration and tactics against our country"; and the addresses of certain military officers assigned to the base.

In a communication to Hernandez from Cuba, Guerrero was directed to "continue with the gathering of military information and at the same time . . . search for new relations and tightening of the ones he already possess [*sic*], with the aim of achieving broader penetration and gathering of information at the base."

Alejandro Alonso

Alejandro Alonso, a.k.a. "Franklyn," resided at 19761 SW 79th Place, Miami and was arrested there in the early morning hours of 12 September 1998. Hernandez handled Alonso.

In the computer records obtained from Hernandez's apartment were expense reports relating to "Franklyn," his telephone and beeper numbers, as well as operational plans and meeting sites involving Alonso. On one occasion when Alonso failed to answer a page by Hernandez in a timely manner, he was admonished and told that he needed to maintain "a full combat readiness status . . ."

Records reflect repeated directions from the Cuban Government that Alonso participate in and report information on the Miami-based Cuban exile group known as *Movimiento Democracia* (to be "the eyes of the [Cuban Government] in the Movimiento Democracia"). A boat pilot, Alonso was directed to and participated in "flotillas" organized by *Movimiento Democracia* in demonstrations against the Cuban Government.

Alonso prepared a detailed account of his observation of a July 1996 flotilla to the waters near Cuba in which he participated as a pilot and gave it to Hernandez for forwarding to the Cuban Government. Alonso's report enumerated persons participating in the flotilla and provided navigational information concerning courses and locations pertinent to the flotilla. Alonso also reported on plans for a "flotilla" demonstration to occur near Cuban waters during the Pope's visit in January 1998 and a proposed concert by a popular singer on boats off the coast of Cuba. Reports by Alonso included patriotic slogans in support of the Cuban regime and critical remarks about the anti-Castro activities he pretended to support in his infiltration efforts.

Rene Gonzalez

Rene Gonzalez, a.k.a. "Castor" and "Iselin," resided at 8000 SW 149th Avenue, Apartment A-403, Miami and was arrested there on 12 September 1998. Gonzalez is a US citizen, born 13 August 1956. Records of cash payments and other expenses relating to "Castor" are in computer diskettes found in Hernandez's apartment. Also found on the diskettes were frequent communications between Hernandez and Gonzalez using computer diskettes.

The computer diskette demonstrated that Gonzalez reported frequently to Hernandez on the activities of anti-Castro political and humanitarian groups and individuals in the Miami Cuban exile community and that Hernandez routinely forwarded this information to Cuba. The diskettes reflected both written and oral reports from Gonzalez to Hernandez using the code name "Iselin". Specifically, Gonzalez was tasked to report on Brothers to the Rescue (BTTR), *Movimiento Democracia, Militares y Profesionales Por La Democracia*, Commandos United for Liberation, PUND (National Democratic Unified Party), *Comision Nacional Cubano*, and the Cuban American Pilots Association.

Cuba told Hernandez that Gonzalez should become "more aggressive" and be "let loose" once his wife arrived in the United States from Cuba. His wife arrived in December 1996, after Gonzalez and Hernandez devised and implemented a cover story to enlist the assistance of unwitting Cuban-American US Congress persons in obtaining the supposed humanitarian release of the wife to the United States.

Gonzalez was generally tasked to report on information relating to the interests of the Cuban Government. He posed as an FBI informant, ostensibly supplying information about alleged drug smugglers as a means to obtain information regarding FBI activities, its agents, and progress of an investigation of interest to Cuba. In one communication to Hernandez, Cuban authorities detail that one purpose of this supposed cooperation with the FBI was to maintain a channel to use, "(i)f it is of interest to us in an emergency to spark an action by the North American government against these people (Cuban exile groups)." Gonzalez, in one report to Hernandez, reported that he "thwarted (his FBI handler) diplomatically, but I left the door open a crack. I think that I was very convincing . . ."

Nilo Hernandez and Linda Hernandez

Nilo Hernandez, a.k.a. "Manolo," and Linda Hernandez, a.k.a. "Judith," are a married couple that resided at 3012 SW 18th Street, Miami, where they were arrested 12 September 1998. (*Editor's comment: To avoid confusing Nilo Hernandez with Geraldo Hernandez, Nilo will be referred to by his code name "Manolo."*) They resided in the Miami area since at least 1992, having relocated from the New York area. Judith was born in the United States but spent her youth in Cuba, returning to that country before Castro's takeover. She returned to the United States in the mid-1980s.

On the basis of searches of the apartment of Hernandez and Labanino, in communications with Cuba, "Manolo" and "Judith" are often referred to collectively as the "Juniors," the "JRSs," or as "Agents." They were asked to jointly undertake

special assignments by Cuba. “Manolo” was a businessman and proprietor, operating export businesses involving the sale of computer peripheral devices and medical testing kits.

On 12 September 1998, “Manolo” admitted knowing Hernandez, claiming it was a social relationship. The FBI had photographed “Judith” meeting with Fernando Gonzalez, a.k.a. Ruben Campa, a.k.a. “Vicky.”

“Manolo” and “Judith,” while subagents reporting to Hernandez, were trusted and reliable agents. In one communication from Cuba, “Manolo” and “Judith” are said to have the military rank of “sublieutenant,” to have worked for the Cuban Government “for a number of years,” and to have maintained positions in the “reserves” and the “militia.”

In taskings from Cuba, the “Juniors” were given special assignments entrusting them with the identities of other Cuban operatives in the United States—a further indication of their elevated status within the spy ring. For example, the computer records reflect that the “Juniors” were to be assigned specifically to conduct countersurveillance or “dry clean(ing)” projects involving a subagent—“throughout the whole operation, you must use the JRSs to dry clean him during the routes from one (telephone) both to another and even at the places themselves”—and to undertake a long-term surveillance mission of two Cuban agents who were thought to be at risk of defection to US authorities.

Among other assignments, “Manolo” was asked to infiltrate CAMACOL, an exile group, and “Judith” was directed to do likewise with ALPHA 66. They were both asked to “conduct an investigation” of a local telecommunications company as well as to develop closer relations with a former employee of the US Navy ultimately to determine his reaction to assisting them by providing information. “Manolo” apparently also provided Hernandez with technical advice regarding computer and software issues.

Hernandez received instructions from Cuba for “Manolo” and “Judith” to carry out assignments involving the mailing of anonymous, misleading, and threatening letters to political figures in the United States, including communication in the guise of an anti-Castro figure threatening a US Senator for his political position. In outlining one such assignment, Cuba directed: “this task should be performed by Manolo as well as Judith and they should stand firm in their security measures, such as avoid leaving fingerprints in the correspondence, deposit them in different areas and mailboxes, stamp with appropriate postage; avoid being seen during the deposit, act in a normal fashion, make the subject of clothing, possible camouflages, etc. Both of these comrades have experience in this type of task and know how to act.”

A court-ordered search of their home revealed the following items, among others: photography development equipment and chemicals; three portable (walkie-talkie) two-way radios; shortwave radios (one portable) with assorted cables and connectors; numerous city and transmit maps for metropolitan US cities, including New York, Miami, Houston, and Las Vegas. Also found were: instructions for routes and meeting places; women’s wigs and hair attachments and temporary hair coloring spray and dyes; contact lenses in different colors; a bag containing a wig and various colored sunglasses; lists of telephone numbers and locations of public pay phones posted on the refrigerator; and a book entitled *Alpha 66 and its Historical Works* dedicated to Linda and signed with the name of Andres Nazario Sargen, the leader of the organization.

A court-ordered search of an automobile registered to “Manolo” revealed, among other things: two minirecorders in the console with adapters to run off the cigarette lighter, a microphone running from a recorder and clipped to the rear-view mirror, and a \$200 receipt for a miniature recorder from Spy World.

Fernando Gonzalez

Fernando Gonzalez, a.k.a. Ruben Campa and a.k.a. “Vicky,” is a Cuban intelligence officer. (*Editor’s comment: To avoid confusion between Fernando Gonzalez and Rene Gonzalez, Fernando will be referred to by his alias Campa.*) In the autumn of 1997, Hernandez was temporarily recalled to Cuba. FBI monitoring revealed a conversation in October 1997 between Hernandez and Labanino discussing the arrival of an associate with Hernandez commenting that, by the end of the week, the famous “Vicky” should be there.

In the spring of 1998, Labanino was temporarily recalled to Cuba, and in the summer of 1998, Labanino was absent from Miami on other missions. Monitoring revealed conversations in April 1998 between Hernandez and Labanino discussing the associate who would substitute for Labanino. The anticipated associate was variously said to be Roberta, Camilo, and Vicky. In these conversations between the two men, Camilo was said to be the same as Vicky, the one with the limp, approximately 175 pounds, with a receding hairline and moustache. FBI physical observation of Campa showed him to have a receding hairline and mustache, although not the limp or estimated 175-pound weight.

On 3 July 1998, Campa telephoned Hernandez and said that he would arrive the next day. Between 5 July 1998 and early September 1998, electronic surveillance revealed frequent conversations, both on the telephone and in Hernandez’s apartment, in which Campa participated. The surveillance included conversations of Campa dictating his arrival 4 July, reading numbers aloud with Hernandez, and discussing with either Hernandez or Labanino the use of diskettes; equipment problems in which “if the recorder skips, it will skip either sending or receiving”; delays in communications; and when and whether they had recently spoken with “la nena” or “mami.”

Surveillance also revealed Campa discussing with Hernandez meetings or conversations with subagents and using the subagents’ codenames. In a July 1998

conversation, Campa and Hernandez discussed a recent conversation with a female associate of “Judith.” Campa was photographed meeting with “Judith.”

Campa and Hernandez also discussed encounters with “Manolo,” “Junior,” and the “Juniors.” In an August 1998 conversation, Hernandez asked Campa if he had a video, which Hernandez wanted to show to a named subagent. On another occasion, Campa was surveilled meeting at a shopping mall with another subagent, who delivered a laptop computer to Campa for needed adjustments.

In a July 1998 conversation, Campa and Hernandez discussed mutual acquaintances, including one who had been in Moscow and gotten in trouble, and the acquaintances’ movements through various elements of the Cuban intelligence establishment, such as “ISRI group,” referring to an intelligence school, and “M-2,” referring to a specific foreign country.

In September 1998, surveillance revealed a number of conversations in which Campa discussed with Hernandez or Labanino the apparent theft of Labanino’s laptop computer from a hotel room. In a 4 September conversation, Campa tells Labanino not to worry and that he would talk to the people at the “university.” Labanino replied that all of the “study materials” were also taken. In another telephone conversation, Campa told Hernandez that the problem is that they took the disks; the whole story is there.

Joseph Santos and Amarylis Silverio

Joseph Santos, a.k.a. “Mario,” a naturalized US citizen, and Amarylis Silverio, a.k.a. “Julia,” a permanent resident alien, are a married couple who resided at 355 NW 72nd Avenue, Apartment 303, Miami, where they were arrested on 12 September 1998. Before arriving in Miami in mid-1996, they resided in New Jersey. Santos had left Cuba for the United States in 1993.

Santos said he was introduced to Hernandez in December 1998 and told that Hernandez would be his superior. He said he and his wife received orders from Hernandez to collect information on the Southern Command. Financial reports

maintained by Hernandez addressed the issue of payments to them. It appears from the records that \$4,800 was originally allocated to them “for operational expenses and financial help,” but that budget was later reduced.

According to the computer records, Santos and Silverio became subagents of Labanino and were sent to Miami specifically to assist him in the penetration of the Southern Command. “Mario and Julia should start working against it, for which instruction has already been given. That they shall both have as their fundamental assignment the penetration of said command.” It was directed that “both comrades should stay apprised and immediately informed, everything there [*sic*], public information or secret.”

Santos was an employee of a food producer in Miami, at a location close to Southern Command headquarters. It was reported that Santos was making “a preliminary study of (the operational situation) in the area where projects of the Southern Command are being carried out, and Julia (is making) another one on the mail (possibly courier) system and its various options . . .” Other computer disks reflect detailed reports, supported by numerous photographs, made by Santo and Silverio on the construction and geography of the Southern Command and its environs. One such report was entitled, “Observations Around the Southcom Installation.”

Five Ring Members Get Plea Bargains

Five members of the Cuban spy ring accepted plea bargains from the prosecution in return for being a prosecution witness at the trial. The first to be sentenced was Alonso who received a seven-year prison sentence on 29 January 2000. He told investigators where to find a fake identity kit—which was hidden inside a leather notebook—a page of code concealed in a false bottom of a lamp, and a pad of water-soluble paper used for secret messages that was inside a stereo speaker.⁵

Santos agreed to become a witness for the US Government against the others, and in return, he and his wife pled guilty in October 1998 to a conspiracy charge of failing to register as a foreign agent. The judge accepted the plea bargain and on 2 February 2000 sentenced Santos to four years in jail.⁶ His wife, Amarylis, received a three-and-a-half-year sentence.

Linda and Nilo Hernandez also agreed to cooperate.

Cuba Gets Christmas Gift From the United States

On 23 December 1998, the United States informed the Cuban Mission to the United Nations that three of its diplomats could pack their bags and permanently go home. Expelled were Eduardo Martinez Borbonnet, first secretary; Roberto Azanza Paez, third secretary; and Gonzalo Fernandez Garay, an attache.

The Remaining Five Members Tried and Convicted

With the plea agreements from five members in hand, the trial began on 7 December 2000 of the remaining five captured ring members. The five were charged with spying on US military installations in South Florida. Gerardo Hernandez was specifically charged with giving the Cuban Air Force the flight plans of unarmed Cuban exile planes that were shot down in 1996 by a Cuban MIG jet. Four members of Brothers to the Rescue were killed when their two planes were shot down. Four other members are still at large and presumed to be in Cuba. The trial took 100 days with breaks and postponements in between. More than 200 pages of coded messages were produced as evidence along with the testimony of the ring members.

In early June 2001, the trial finally went to a Federal jury. In the end, all five were convicted of spying for Havana. The federal jury found the defendants guilty of operating as foreign agents and conspiring to penetrate US military bases. The spy ring’s leader, Hernandez, was also convicted of involvement in the

Cuban shootdown in 1996 of two unarmed planes operated by Cuban exiles over the Florida Straits.

Hernandez, Labanino, and Guerrero were sentenced to life in prison. Fernando Gonzalez and Rene Gonzalez received lesser sentences. Defense attorneys declined to comment upon leaving Miami's Federal Courthouse. During the trial, the lawyers maintained their clients' primary mission was to monitor what they termed exile extremists who had violated Cuban airspace in the past and backed terrorist campaigns on the island.

Endnotes

¹ *Sun-Sentinel*, 8 June 2001.

² *Ibid.*

³ MacShan, Angus, "Alleged Cuban Spies had Escape Plan, Attorney Says," Reuters, 16 September 1998.

⁴ *Sun Sentinel*, 18 June 2001.

⁵ "Confessed Cuban Spy Received Seven Years," *Miami Herald*, 20 January 2000.

⁶ *Miami Herald*, 11 January 2001.

Brian P. Regan

The FBI arrested Brian P. Regan—a retired US Air Force cryptanalyst—as he cleared security at Dulles Airport on 23 August 2001. Regan was scheduled to board a Lufthansa flight for Zurich, Switzerland.



Regan is 30 years old and lived in Bowie, Maryland. He is married and has two daughters and two sons. He served in the US Air Force from August 1980 until retiring in August 2000. His training in the Air Force included cryptanalysis. His responsibilities included the administration of an Intelink Web site—a classified US Government computer system accessible only by certain members of the US Intelligence Community.

Regan's last assignment with the Air Force was at the headquarters of the National Reconnaissance Office (NRO) in Chantilly, Virginia. During Regan's Air Force assignment at the NRO, he had access to classified US national defense information up to the Top Secret level and also had access to sensitive compartmented information (SCI). His access to SCI was terminated when he retired from the Air Force on 30 August 2000.

Regan was employed by TRW in Fairfax, Virginia, in October 2000. On 25 July 2001, his SCI access was reinstated allowing him to return to the NRO as a TRW contractor on 30 July 2001.

In the fall of 2000, a reliable source indicated that a number of US Government documents had been provided to the government of Country A, which the *Washington Post* identified as Libya. The large majority of these documents were classified and related to the US national defense. These documents were not authorized for release to Country A. The remaining documents were portions of classified documents—the portions are unclassified, but the documents in their entirety were not authorized for release to Country A.

Most of the classified documents provided to country A consisted of electronic images classified Secret that were taken from overhead platforms. Another document consisted of classified portions of a CIA intelligence report classified Secret and issued on a specific date. The particular copy of this report provided to Country A had been printed out eight days after the date the report was issued. Another of the documents consisted of two classified pages from a CIA newsletter that is classified Secret overall.

Among the other documents passed to country A were the following:

1. A Secret document relating to a foreign country's satellite capability.
2. The unclassified cover page of a defense intelligence reference document classified Top Secret.
3. One page from a document containing Top Secret information.
4. The unclassified table of contents for a particular intelligence manual classified Top Secret.

The documents also included two photographs—one classified Secret and the other classified Confidential.

Also, in the fall of 2000, a reliable source revealed that an agent had provided the government of Country A with separate information intended to accompany the documents described above. This accompanying information consisted of an introductory message,

in English, which contained instructions to prevent detection of the messages by the US Government along with separate encrypted messages.

The encrypted messages, which were decrypted by the US Government, set forth contact instructions, established bona fides, and offered to provide additional classified information. In particular, the encrypted message gave instructions to respond to a specified e-mail address on a free e-mail provider. A “Steven Jacobs,” of a specific address in Alexandria, Virginia, ostensibly established this e-mail address.

Records of the provider indicate that this e-mail address was established on 3 August 2000 and was accessed nine times between August 2000 and January 2001. Eight of the nine times this e-mail address was accessed were from public libraries located in Anne Arundel and Prince George’s Counties, Maryland. Regan’s residence is located one-half mile from a Prince George’s County library with public Internet access.

One of the Anne Arundel County libraries used to access this account is in Crofton, Maryland, approximately five miles from Regan’s residence. Physical surveillance of Regan during May through August 2001 indicated that Regan regularly utilized the public Internet access located in the Crofton library. The ninth access to the address occurred at the Tysons-Pimmit Library in Falls Church, Virginia, which is located along the route Regan used to commute between his residence and his NRO office.

The FBI searched the office formerly occupied by Regan at the NRO in April 2001. A copy of the intelligence manual referred to above (bullet number 4), bearing Regan’s name, was found on a shelf behind his former desk.

The FBI also searched the computer formerly assigned to Regan at the NRO in April 2001. FBI special agents analyzed the hard drive of this computer and found that someone using Regan’s password had surfed a large number of Intelink Uniform Resource Link (URL) addresses pertaining to countries A, B, and C.

One of these URL addresses is for one of the overhead images discussed above. Also on the hard drive of Regan’s computer were four URLs that corresponded to the URL addresses containing direct links to some of the other documents above. In addition, NRO server records indicate that Regan’s computer was used to gain access to three of the other compromised documents.

Intelink audit records indicate that the URL for the CIA intelligence report was accessed from the computer in Regan’s former office at 8:52 p.m. on the date the particular copy of the report had been printed out. NRO records indicate that Regan’s electronic entry badge was used to enter his office suite at 1:55 p.m. on that date. The FBI also established that there were common spelling errors in the messages and in documents typed on Regan’s NRO computer.

The CIA intelligence report, which related to a foreign country’s satellite capability, was composed expressly for and distributed at a course given at Colorado Springs, Colorado, that Regan attended 28 July through 8 August 1997. The course was given for cleared members of the US Intelligence Community—Regan was one of two NRO members who attended the course. Regan was the designated recipient at the NRO for all classified materials distributed at the course.

Separate NRO security records indicate that Regan’s passcode was used to set the alarm on the suite at 1:15 a.m. the following morning. Later that same day, Regan flew on a “space available” US Air Force flight from Norfolk, Virginia, to Iceland, and thereafter traveled to additional locations in other European countries.

The FBI has had Regan under surveillance since June 2001. On several occasions while under surveillance, FBI personnel observed Regan conducting what appeared to be surveillance detection runs; that is, conducting multiple U-turns, pulling over to the side of the road, and appearing to check to see whether he was under surveillance.

In early June 2001, FBI surveillance observed Regan log onto the Internet at a public library. When Regan departed, FBI personnel noted that he had failed to sign off the Internet, and they were able to observe which Internet sites Regan had visited. One of the sites that Regan had visited provided the address for a diplomatic office of Country C in Switzerland. Regan had also looked up a hotel in Zurich.

On 21 June 2001, Regan sent an e-mail from an account registered in his own name to an e-mail account in his wife's name. The e-mail attached one page of an alphanumeric encryption key that appears to be similar to the encryption technique described above.

On 26 June 2001, Regan traveled from Washington Dulles International Airport to Munich, Germany, on Lufthansa. Before Regan's flight departed, the FBI searched his checked suitcase, pursuant to a court order. Regan's suitcase contained glue and packing tape. Regan returned to Washington on 3 July 2001.

On 23 August 2001, at approximately 9:00 a.m., while Regan was occupied in a meeting at NRO, the FBI conducted a court-authorized search of Regan's Dodge Caravan. In that search, the FBI found a carry-on bag, which contained four pages of what appeared to be handwritten encrypted messages—one page of which appeared to be a typewritten encrypted message and another page that may be one page of a decryption key. The carry-on bag also contained handwritten addresses and phone numbers for diplomatic offices of Country D in Bern, Switzerland, and Vienna, Austria, and for a diplomatic office of Country C in Vienna. On the same day, the FBI also searched—pursuant to a court order—Regan's brown suitcase. In that suitcase were a bottle of Elmer's glue and a roll of tape. Also on 23 August, the FBI conducted surveillance of Regan's office at the NRO by closed circuit television, pursuant to a court order. He was observed looking at a Secret document on his computer terminal while taking notes in a small notebook that he took from, and returned to, his front pants pocket. A court-authorized search of Regan's computer confirmed that he had been logged onto Intelink accessing classified material.

Regan had reservations to Zurich, Switzerland, through Frankfurt, Germany, on Lufthansa, departing from Washington Dulles on 23 August 2001—which he reconfirmed on 11 August 2001—and returning on 30 August 2001. On 23 August 2001, Regan told a coworker that he was driving to Orlando, Florida, to take his family to Disney World, leaving on 27 August and returning 30 August. In addition, Regan wrote "Orlando, Florida" on a dry-erase board in his office suite, indicating to his colleagues where he would be for this time period. Regan did not report to his employer that he would be traveling outside the country, which he was required to do under NRO regulations concerning foreign travel by personnel having security clearances.

Later on 23 August, Regan drove to Dulles Airport, arriving at approximately 1:00 pm and checked a brown suitcase at the Lufthansa counter. This suitcase was secured by and is in the custody of the FBI. After Regan was bumped to a later flight, he departed Dulles Airport and returned to his NRO office. Regan drove back to Dulles Airport at approximately 5:30 p.m. and was stopped by the FBI in the airport terminal. Regan had the same carry-on bag containing the same documents that were found in the FBI search of his van earlier in the day.

Also in Regan's carry-on bag when the FBI stopped him was an NRO document marked For Official Use Only that listed classes available to members of the US Intelligence Community. This document indicated the security clearance required to attend each class. This document consisted of two pages—front and back—and FBI personnel had earlier observed Regan (via court-authorized closed-circuit television) create this document by cutting and taping together documents and then photocopying the taped-up document. When he was stopped, Regan was also carrying: approximately five blank business-sized envelopes, three rubber gloves, and four finger sleeves.

Regan's carry-on bag also contained a hand-held global positioning system (GPS), which can be used to locate a specific site for use as a deaddrop or as a signal site. He also had a spiral notebook

that appeared to be the notebook in which he was taking notes while looking at classified information on his computer terminal earlier in the day. In addition, hidden in Regan's shoe, was a piece of paper on which was written names and addresses in a European country.

FBI special agents at the airport confronted Regan at approximately 5:35 p.m. In response to a question, Regan denied knowledge of cryptology, coding, and decoding. However, when shown photographs of the cryptology-related alphanumeric tables—tables that had been in his carry-on bag—he stated, “This is my stuff.” Regan was arrested shortly thereafter.

Financial checks indicated that, in February 2001, Regan had consumer debts amounting to \$53,000.

Avery Dennison

On 28 April 1999, FBI Director Louis J. Freeh announced that a guilty verdict was reached against a Taiwanese businessman, his daughter, and his company in connection with the theft of trade secrets from Avery Dennison, an Ohio manufacturing facility. Avery Dennison is a subsidiary of Avery Dennison Corporation—one of the nation's largest manufacturers of adhesive products—Pasadena, California. The company employs some 16,000 people worldwide.

Director Freeh stated, “This case marks one of the first convictions of foreign individuals under the Economic Espionage Act of 1996, which has gone to trial. It is also the first case in which a foreign company was charged and found guilty of an Economic Espionage violation.”

A Federal jury convicted Pin Yen Yang, Chairman of Four Pillars Enterprise Co, Ltd.; Yang Hwei Chang, a.k.a. Sally Yang, a company executive; and their company of two counts of violation of Title 18, USC, Section 1832 (a)(4), Attempted Theft of Trade Secrets, and Title 18, USC, Section 1832 (a)(5), Conspiracy.

Director Freeh pointed out that Avery Dennison Corporation provided extensive assistance to the FBI since the inception of this investigation. It was Avery Dennison who, through its own internal investigation, first uncovered evidence of economic espionage and then turned it over to the FBI. Freeh said, “This investigation and conviction clearly demonstrate the importance and value of law enforcement and industry working in partnership under the Economic Espionage Act to combat the theft of American trade secrets and jobs by foreign business interests. It is essential that this partnership continue to adequately combat a crime, which has such an impact on the economic well-being of this nation.”

FBI agents arrested Yang and his daughter, Hwei Chang, on 5 September 1997 at Hopkins International Airport in Cleveland, Ohio. They were traveling to New York to see the US Open

tennis championship. Both were charged with mail and wire fraud, conspiracy to steal trade secrets, money laundering, and receipt of stolen goods from the Avery Dennison. The pair was arrested after negotiating with an employee of Avery Dennison to obtain additional trade secrets. That employee was cooperating with the FBI in an undercover capacity. Since July 1989 the defendants had obtained, among other things, Avery Dennison trade secret information relating to formulations for self-adhesive products.

Federal prosecutors said an initial estimate regarding the search and development costs expended by Avery Dennison to develop the information obtained by the defendants could exceed between \$50 million and \$60 million.

Yang is the president of Four Pillars Enterprise Company, Ltd., of Taiwan, which manufactures and sells pressure-sensitive products mainly in Taiwan, Malaysia, Singapore, the United States, and the People's Republic of China. Avery Dennison is one of Four Pillars' chief competitors in the manufacture of adhesives. There was no indication that individuals from the People's Republic of China participated in the scheme.

Hwei Chen is a corporate officer of Four Pillars, which has more than 900 employees and annual revenues of more than \$150 million. She is believed to hold dual citizenship in the United States and Taiwan. Four Pillars previously employed Hwei Chen, who has a Ph.D. in analytical chemistry from New Mexico State University, as an Applied Research Group Leader.

A 21-count indictment was returned in US District Court in Cleveland on 1 October 1997. The indictment alleges that from July of 1989 through 1997 the defendants Yang, Hwei Chen, and Four Pillars Enterprise engaged in a scheme to defraud Avery of the intangible right to the honest service of Dr. Victor Lee and of its confidential and proprietary information and trade secrets.

Dr. Lee, a native of Taiwan, was employed by Avery in 1986 to do scientific research into

adhesives. At all times relevant to this case, Lee was an employee of Avery. In 1989, while Lee was making a presentation in Taiwan, Four Pillars vice-president C.K. Kao introduced him to Yang and Sally. Yang asked Lee to serve as a "consultant" to Four Pillars and offered him compensation of \$25,000 for a year of consultation. The parties agreed that they would keep the arrangement secret. Lee received a check, made out to his sister-in-law, from Four Pillars shortly thereafter.

After his return to the United States, Lee corresponded with Yang and Sally, describing the information he would provide them and indicating that some of the information Lee intended to provide the Yangs was confidential to Avery. On 8 August 1989, Lee sent two confidential Avery rheology¹ reports to the Yangs. The Yangs responded that the information was very helpful.

Lee continued to supply the Yangs with confidential information, including information that Four Pillars could use in making a new acrylic adhesive developed by Avery. The Yangs sent Lee samples of the adhesives they had created using information he had supplied; Lee tested the samples and offered comparisons with Avery's products derived from the same adhesive formula.

The FBI confronted Lee after learning of Lee's industrial espionage. Lee admitted his relationship with the Yangs and Four Pillars and provided the government with materials documenting his activities since 1989. Lee also agreed to cooperate with the government in a sting operation to arrest and prosecute the Yangs. A short time later, Yang told Lee that he would be in the United States during the summer of 1997. Lee volunteered that he had information on a new emulsion coating that he would provide Yang at that time and asked whether Yang might also be interested in information on Avery's operations in Asia. Yang was very interested.

On 4 September 1997, Lee met Yang and Sally in Lee's hotel room in Westlake, Ohio. Lee had consented to the FBI's videotaping this meeting. In the course of the meeting, Lee showed the Yangs

documents provided by the FBI, including an Avery patent application relating to a new adhesive product. The documents bore “confidential” stamps, and Lee emphasized to the Yangs that the information was the confidential property of Avery. Yang and Sally, at Yang’s direction, began to tear off the “confidential” stamps. The Yangs discussed with Lee the information Lee had previously provided to Four Pillars. The Yangs were arrested the next day.

Victor Lee, age 47, of Concord, Ohio, and a US citizen, pleaded guilty to a one-count information wire fraud charge. The charge alleges that Lee, who was employed by Avery in Concord, Ohio, as research engineer, disclosed confidential and proprietary information belonging to Avery to Four Pillars. The plea agreement between the government and Lee requires Lee to cooperate fully with the federal prosecutors in all matters relating to the ongoing investigation and prosecution of Four Pillars, P.Y. Yang, and H.C. Yang.

Prior to the conclusion of the trial, the District Court disposed of all but one of the fraud counts and all of the money laundering and receipt of stolen property counts. On 29 April 1999, the jury found the Defendants guilty of attempt and conspiracy to commit theft of a trade secret and acquitted them on the remaining fraud charge.

During the course of the proceedings, the Defendants made numerous motions, including pretrial motions to suppress evidence—a *Batson* challenge to the composition of the jury—and motions for mistrial on several grounds, all of which the District Court denied. In September 1999, the Defendants moved for a new trial and renewed their motions for mistrial. After an evidentiary hearing on these motions, the court denied each of them.

On 5 January 2000, the Defendants were sentenced. The court departed downward 14 levels in establishing the offense level for each of the Defendants; the court, however, departed upward in sentencing Four Pillars, imposing the statutory maximum fine of \$5 million. The

Defendants appealed the denial of their pretrial, trial, and post-trial motions and the District Court’s upward departure in imposing Four Pillars’ fine. The government appealed the District Court’s downward departure for each Defendant.

The principal issues in the appeal were the Defendants’ contention that under the circumstances of this case it was legally impossible for them to have committed the crimes of which they were convicted; Four Pillars’ contention that the District Court erred in departing upward in imposing sentence; and the government’s contention that the District Court erred in departing downward in setting the offense levels of the Defendants. In addition, the Defendants challenge the District Court’s denials of a motion to suppress video- and audiotape evidence, a *Batson* challenge, a motion to prohibit contact between prosecutors and witnesses, motions for mistrial because of alleged prosecutorial misconduct, and motions for new trial on grounds of newly discovered evidence. Finally, the Defendants claim that the District Court’s instruction on the meaning of “theft” was plainly erroneous and that the evidence did not support their convictions.

On appeal the Defendants argued that the District Court erred when it ruled that the government did not have to prove that what the Defendants sought to steal was an actual trade secret. The Defendants contended that the District Court’s reliance on *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998), which held that legal impossibility is no defense to attempt and conspiracy charges, was error because *Hsu* was incorrectly decided.

The court reviewed de novo, the District Court’s definition of the elements of the charged offense, the meaning attached to those elements, and the applicability of the defense of legal impossibility.² In *Hsu*, the Third Circuit was faced with a claim nearly identical to that raised by the Yangs, namely, that it was legally impossible for the defendants to be guilty of attempting to steal a trade secret and conspiring to steal a trade secret because that which they were accused of attempting and conspiring to steal was not, as it turned out, an

actual trade secret. This issue arose in the context of the defendants' claim that they were entitled to examine the trade secret documents in order to establish their defense of legal impossibility because, in their view, if those documents did not actually contain trade secrets, then the defendants could not be guilty of attempting to steal trade secrets. Hsu was one of several individuals led to believe that a scientist employed by Bristol-Myers Squibb, who was secretly cooperating with the FBI, was willing to sell corporate secrets.³ A meeting was arranged at which Hsu met with the scientist and personally reviewed and discussed with him Bristol-Myers documents that were clearly marked "CONFIDENTIAL."⁴ Immediately thereafter, the FBI arrested Hsu.⁵

Hsu was charged with attempt and conspiracy to steal a trade secret under 18 U.S.C. § 1832. He was not charged with the actual theft of a trade secret. Hsu claimed that, if that which he had sought to steal was not in fact a trade secret, it was legally impossible for him to be guilty of the offense of attempted theft of a trade secret. The Third Circuit rejected this defense. The court noted that virtually no other circuit continued to recognize the defense of legal impossibility and that even in the Third Circuit the defense had been severely limited. In particular, the court reviewed its holding in *United States v. Everett*, 700 F.2d 900 (3d Cir. 1983), that legal impossibility is not a defense to the charge of attempted distribution of a controlled substance under 21 U.S.C. § 846. Consistent with the analysis in *Everett*, the *Hsu* Court reviewed the legislative history of the EEA, particularly the comprehensive nature of the law's approach to the serious and growing economic threat presented by corporate espionage, and the fact that the law was drafted at a time when the defense of legal impossibility had been almost entirely abandoned.⁶ The court also observed that, if it were to hold that legal impossibility is available as a defense to the charge of attempted theft of trade secrets, the anomalous result would be that the government would be compelled to use actual trade secrets in its sting operations and would be compelled to turn over those trade secrets to the persons charged with attempting to

steal them. Accordingly, the court concluded that legal impossibility is not a defense to a charge of attempted theft of trade secrets. Rather, the court held that a defendant is guilty of attempting to misappropriate trade secrets if, "acting with the kind of culpability otherwise required for commission of the crime, he . . . purposely does or omits to do anything that, under the circumstances as he believes them to be, is an act or omission constituting a substantial step in a course of conduct planned to culminate in his commission of the crime."⁷ Because the defendant's guilt turns on the "circumstances as he believes them to be," the court held that the government was not required to prove that what the defendant sought to steal was in fact a trade secret, but only that the defendant believed it to be one.

Turning to the charge of conspiracy to steal trade secrets, the Third Circuit held that legal impossibility is not a defense to the charge of conspiracy to steal trade secrets. The court held that the basis of the conspiracy charge is the agreement to commit the unlawful act and not the unlawful act itself. Therefore, because the "illegality of the agreement does not depend upon the achievement of its ends," and because it is "irrelevant that the ends of the conspiracy were from the very inception of the agreement objectively unattainable,"⁸ it is also irrelevant that it may have been objectively impossible for the conspirators to commit the substantive offense. Accordingly, the court held that, because legal impossibility is not a defense to the charge of conspiracy to steal trade secrets, the government was not required to prove that the information the defendants conspired to steal was in fact a trade secret.

The Appeals Court found the logic and reasoning of the Third Circuit persuasive. It did not feel it necessary to delve into the question of whether a defense of legal impossibility was recognized at all in the Sixth Circuit, and indeed, was aware of a handful of cases over the past decade in which the court had at least acknowledged the possibility that there is such a defense.⁹ Importantly, the Appeals Court, like the Third Circuit, had definitively established in the context of the federal drug laws

that impossibility is not a defense. In *United States v. Reeves*, 794 F.2d 1101 (6th Cir. 1986), the court determined that, in light of the congressional desire to enforce federal drug laws as fully as possible, the fact that the defendant did not actually possess or gain possession of cocaine (but instead possessed an innocuous substance) was irrelevant to the defendant's conviction for attempt to distribute and possess cocaine because attempt requires that the government establish (1) an intent to engage in criminal activity, and (2) the commission of an overt act constituting a substantial step toward the commission of the substantive offense. Since neither element required the completion of the substantive offense, or that the material object of the defendant's desires (cocaine or a sham substance) actually be illegal, the court concluded that the defendant was guilty of attempted distribution and possession of cocaine.

Further, like the Third Circuit, the Appeals Court maintained that congressional purpose gives meaning to the extent and reach of a statute.¹⁰ Here, the purpose of the EEA was to provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets. To follow the Yangs' reasoning and rule as they ask would eviscerate the effectiveness of the act. The government would be severely limited in its ability to use the assistance of people willing to cooperate to catch and convict thieves of trade secrets. In effect, the Yangs' position would, as the Third Circuit pointed out, force "the government to disclose trade secrets to the very persons suspected of trying to steal them, thus gutting enforcement efforts under the EEA."

Under the Model Penal Code a defendant is guilty of attempting to commit a criminal offense when he "purposely does or omits to do anything that, under the circumstances as he believes them to be, is an act or omission constituting a substantial step . . . planned to culminate in his commission of the crime."¹¹ The Yangs believed that the information Lee was providing was trade secrets belonging to Avery. They attempted to steal that information. The fact that they actually did not receive a trade secret is irrelevant. Since the Yangs intended

to commit the crime and took a substantial step toward commission of the crime, they violated §1832(a)(4).¹²

The Yangs' conspiracy to steal the trade secrets in violation of §1832(a)(5) was completed when, with the intent to steal the trade secrets, they agreed to meet with Lee in the hotel room and when they took an overt act toward the completion of the crime, that is, when the Yangs went to the hotel room. The fact that the information they conspired to obtain was not what they believed it to be does not matter because the objective of the Yangs' agreement was to steal trade secrets, and they took an overt step toward achieving that objective. Conspiracy is nothing more than the parties to the conspiracy coming to a "mutual understanding to try to accomplish a common and unlawful plan,"¹³ where at least one of the conspirators knowingly commits an overt act in pursuit of the conspiracy's objective.¹⁴ It is the mutual understanding or agreement itself that is criminal, and whether the object of the scheme actually is, as the parties believe it to be, unlawful is irrelevant.

In sum, we adopt the reasoning employed by the Third Circuit. The Appeals Court affirmed the District Court's ruling that legal impossibility is not a defense to prosecution under §1832(a)(4) and (5).

The District Court made a number of sentencing departures, which are challenged on appeal. The District Court departed downward 14 levels in setting the adjusted offense level for each of the Defendants. The District Court then departed upward and imposed the statutory maximum fine of \$5 million on Four Pillars. The District Court later denied Four Pillars' motion for correction of sentence pursuant to Federal Rule of Criminal Procedure 35(c).

The Sentencing Guidelines, referencing 18 U.S.C. §3553(b), permit a downward departure when "there exists an aggravating or mitigating circumstance . . . not adequately taken into consideration by the Sentencing Commission."¹⁵ The Appeals Court reviewed the District Court's departures from the recommended Sentencing

Guidelines for abuse of discretion.¹⁶ That standard included a review to ensure that the factors upon which the District Court based its decision to depart are a permissible basis for departure—a question of law—since a District Court abuses its discretion when it makes an error of law. Whether the factors are a permissible basis for departure is a question of law. A reviewing court owes no deference to the sentencing court’s resolution of that question.

In deciding whether to depart, the sentencing court must determine whether the factors possibly warranting departure are forbidden, encouraged, or discouraged by the Sentencing Commission.¹⁷ If the sentencing court determines that those factors are permissible and warrant a departure, the court must also provide a statement of reasons sufficiently detailed to permit review of the reasonableness of the departure in light of the grounds for it.¹⁸

The District Court issued a memorandum of opinion explaining the sentences. In that opinion, the court’s primary justification of its 14-point departure for each of the three Defendants was Avery’s participation in the prosecution, about which the court said, “In my experience no victim has played a more direct role than Avery in prosecuting a criminal case. . . . With Avery’s participation and the acquiescence of the Government, the criminal case has become a tool for Avery to seek vengeance instead of a pursuit of justice.” The District Court chastised Avery for “ha[ving] been an active participant in, and at times, even manipulated, the presentation of the Government’s case to enhance its ability to recoup its losses,” and for “attempting to control the sentence” through the calculation of the loss suffered as a result of the Defendants’ activities. Other than Avery providing to the government the same loss evaluation experts Avery intended to use in the parallel civil case against the Yangs, however, the court pointed to no instances or examples of Avery’s “manipulation” or “control” of the trial or the sentencing. Neither did the court provide any insight into how or why Avery’s participation lessened the Defendants’

culpability or the seriousness of their crime, or how Avery’s participation in the prosecution in any way constituted an “aggravating or mitigating circumstance of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission.”¹⁹

It is unlikely that in determining the applicable sentences for theft of trade secrets—or for any other offense, for that matter—the Sentencing Commission took into consideration the participation of the victim in the prosecution of the crime. Certainly it is not mentioned as a factor whose consideration is forbidden in determining whether to depart from the applicable Sentencing Guidelines. The reason for the omission is, we suspect, that the victim’s participation in the prosecution is wholly irrelevant to either the defendant’s guilt or the nature or extent of his sentence. While the Appeals Court did not dispute the Defendants’ contention that *Coleman*, 188 F.3d at 358, prohibits the District Court from categorically excluding any nonprohibited factor from consideration in determining whether to make a downward departure, the court was also aware of the Supreme Court’s reminder that if a factor is unmentioned in the Guidelines, the court must, after considering the “structure and theory of both relevant individual guidelines and the Guidelines taken as a whole,” decide whether it is sufficient to take the case out of the Guideline’s heartland. The court must bear in mind the Commission’s expectation that departures based on grounds not mentioned in the Guidelines will be “highly infrequent.”²⁰

Consideration of the structure and theory of the Guidelines as a whole requires that the court look at the factors to be considered in imposing sentence, as set forth in 18 U.S.C. § 3553(a). None of those factors in any way implicates a consideration of the participation by the victim of the crime in the prosecution of the offender. The structure and theory of the Guidelines as a whole includes the provisions of 28 U.S.C. § 994, which lays out the duties of the Sentencing Commission. Subsections 994 (c) and (d) each lists factors to be considered by the Commission in establishing

categories of offenses (§994(c)) and categories of defendants (§994(d)) for use in the Guidelines and policy statements. Those subsections mandate that the Commission consider whether the listed factors, among others, “have any relevance to the nature, extent, place of service, or other incidents . . . of an appropriate sentence, and shall take them into account only to the extent that they do have relevance.”²¹ None of the factors in either subsection remotely implicated the participation of the victim in the prosecution of the offender. More importantly, however, those subsections made it clear that the factors the Commission was to consider must be relevant to the offense or the offender. The District Court provided no explanation of how the victim’s participation in the prosecution was in any way relevant to either the offense or the offenders.

The Supreme Court made it clear in *Koon* that the issue in sentencing departures is not “whether the particular factor is within the ‘heartland’ as a general proposition, but whether the particular factor is within the heartland given all the facts of the case.”²² The District Court provided no basis upon which the Appeals Court could conclude that Avery’s participation in the prosecution of these Defendants takes this case outside the “heartland” of Guidelines cases. Accordingly, the Appeals Court concluded that the District Court abused its discretion in departing downward on this basis.

Contrary to the Defendants’ claims, the District Court did not base its 14-level downward departures on a series of “unquantifiable factors.” The District Court based its departures primarily on its perception that Avery had improperly participated in the prosecution of the offense and additionally on its concern that the government had overcharged the Defendants, that the Defendants’ conduct dating back to the inception of the scheme to steal Avery’s confidential and proprietary information was not illegal at the time, and that the government was using that conduct to enhance the Defendants’ sentences. The participation of Avery in the prosecution of the Defendants the Appeals Court had already concluded was not relevant to the sentencing of these Defendants and,

at least in this case, was not a permissible basis for downward departure. The District Court conceded in the sentencing order that the Defendants were not convicted on any of the counts that constituted overcharging. Finally, if the District Court believed that the conduct in the counts on which the Defendants were acquitted and the pre-EEA theft of Avery’s proprietary information was not relevant conduct and should not be considered in calculating the sentence, the court should have refused to consider it in arriving at the initial offense levels. Instead, however, the court expressly characterized that conduct as relevant conduct and included it in its calculations of loss as well as its determinations of more than minimal planning and role in the offense. If that conduct was relevant for purposes of determining the offense levels and amount of loss, the Appeals Court was at a loss to understand how its consideration can at the same time be the basis for a downward departure.

The Appeals Court held that the District Court abused its discretion in departing downward 14 levels for each of the Defendants. It noted as well that, although the Pre-sentence Reports contained mention of possible grounds for downward departure, the reports did not mention any of the grounds that the District Court in fact relied upon in making these very significant departures. The District Court’s failure to give notice of its intention to depart, we conclude, was error as well.²³

The District Court, after departing downward 14 levels to an adjusted offense level of six for Four Pillars, for which the fine would have been \$5,000, *see* USSG § 8C2.4(d), or a maximum of \$16,000, *see* USSG § 8C2.6, fined Four Pillars the statutory maximum of \$5 million. Citing USSG § 5E1.2(d)(1) and 5E1.2 cmt. n.4, the court denied Four Pillars’ motion to correct its sentence. The court stated summarily that the Guideline maximum was insufficient to punish, deter, prevent a windfall, and reflect the seriousness of the crime.

The reasons offered by the District Court for the extent of the upward departure were insufficient. A District Court when departing must cite to

facts and circumstances that justify the extent of the departure.²⁴ The size of the departure should correspond to the grounds for the departure. Here, the District Court merely recited sections from the Guidelines and then concluded that \$5 million was the appropriate fine. Furthermore, the Appeals Court found it very difficult to reconcile the 14-level downward departure in offense level with the upward departure necessitated by that downward departure in order to arrive at a fine that, in the District Court's opinion, adequately accomplished the objectives of the Guidelines.

The Appeals Court then vacated the sentences of all Defendants and remanded this matter to the District Court for resentencing consistent with its opinion.

The Defendants, as alluded to above, assign as error a variety of the District Court's orders entered during the course of the proceedings, including (1) denial of a motion to suppress the video- and audiotapes of the hotel room meeting, (2) overruling of a *Batson* challenge to the composition of the jury, (3) denial of a motion to disallow contact between the prosecutors and witnesses, (4) denial of a motion for mistrial based on prosecutorial misconduct, and (5) denial of a motion for a new trial based on newly discovered evidence. The Defendants further claim that the District Court plainly erred in its instruction to the jury on the meaning of "theft" and that the evidence is insufficient to support their convictions. As explained below, the Appeals Court found no merit to these claims.

Sally Yang claimed that denial of her motion to suppress the tapes made by the FBI of the Yangs' meeting with Lee in his hotel room was error. She contended that the taping was unconstitutional because the FBI did not obtain a warrant; further, she claimed that because the tapes included some very brief periods when Lee was not in the room, the taping violated 18 U.S.C. § 2511(2)(c). The Appeals Court reviewed for clear error the District Court's factual determinations with regard to the motion to suppress; it reviewed de novo the court's legal determinations.²⁵

The FBI was not required to obtain a warrant because it had Lee's consent to videotape the meeting.²⁶ The Yangs voluntarily came to the meeting with Lee and voluntarily talked with him in his hotel room. They had relinquished any "justifiable" expectation of privacy.²⁷ The Appeals Court found no merit to Sally's claim that the entirety of the tapes must be suppressed because they contain brief periods when Lee was not in the room. The record establishes that the technicians taping the meeting were expressly instructed to tape only while Lee was in the room. The technicians erred. The record establishes that the prosecutors learned of this error and, without reviewing the tape, arranged for the unauthorized time periods to be redacted. The un-redacted version was made available to the Defendants, but nothing from the unauthorized time period was ever utilized in the prosecution. Further, the District Court, after an evidentiary hearing, concluded that the government had not acted in bad faith. The Appeals Court found no error here.

The Yangs then claimed that the government exercised its peremptory challenges in a discriminatory manner in violation of the Equal Protection Clause.²⁸ Specifically, the Yangs contend that, because the government excluded three women—two of whom were black—in exercising three peremptory challenges, the government was excluding jurors on the basis of race and gender. The Appeals Court reviewed for clear error the factual findings upon which the District Court based its ruling.²⁹

To establish a violation under *Batson*, the defendant must make a prima facie case by showing that the government removed jurors for a discriminatory reason.³⁰ The burden of production then shifts to the government to offer a race- (or gender-) neutral justification for its challenges.³¹ At this stage, the government's explanation need not be "persuasive, or even plausible," but it must simply be one in which discriminatory intent is not inherent. The final step is for the trial court to determine whether the party challenging the peremptory strikes has proven purposeful discrimination. Here, the District Court may decide to disbelieve

an implausible or silly reason, but the burden is on the party challenging the strike to prove that it was motivated by discriminatory animus. The final makeup of the jury is relevant to a finding of discrimination.³²

In response to the Defendants' *Batson* challenge, the government claimed that it struck one juror because of an apparent "attitude problem," a second because she was unemployed, and a third because she did not have the necessary background to be a juror. The District Court found those explanations to be legitimate and race and gender neutral. Following this ruling, the government did not use its remaining challenges, and the final jury consisted of nine women and five men. The Appeals Court concluded that the reasons offered by the government for its peremptory challenges do not violate equal protection. The Yangs showed neither purposeful discrimination nor that the government's reasons were illogical.

The Yangs argued that the District Court erred when it denied their motion to prevent the prosecutors from having contact with the witnesses whom the prosecution was allegedly coaching. The grant or denial of such a motion is within the sound discretion of the District Court.³³ The Yangs cross-examined the allegedly coached witnesses and commented on the alleged coaching to the jury in their closing arguments.³⁴ After reviewing the record, the Appeals Court found that the District Court did not abuse its discretion.

The Yangs further appealed the District Court's denial of their motion for a mistrial based on prosecutorial misconduct. For example, the Yangs contend that a prosecutor attempted to improperly influence a juror by making eye contact, smiling, and nodding at the juror as she entered the room. The Yangs also assert that this juror was particularly receptive and attentive during the prosecution's closing argument, while unreceptive to the Defendants' closing arguments. Another instance of misconduct was said to have occurred when a prosecutor was making head gestures while the defense was examining a witness. Finally, the Yangs alleged a number

of examples of the prosecutors' vouching for and improperly bolstering witnesses' credibility, improperly commenting on the lack of evidence, and wrongfully attacking the defense counsel's character.

The Appeals Court reviewed for abuse of discretion the District Court's denial of a motion for mistrial.³⁵ The District Court denied the Yangs' motions for mistrial and, after extensive discussion, found that "this whole thing . . . has been blown out of proportion." The court, therefore, refused to hold a *Remmer* hearing.³⁶ A *Remmer* hearing is not required unless the defendant can show that the unauthorized juror contact "created actual juror bias."³⁷ The Yangs' failed to offer evidence sufficient to support a finding that the alleged juror contact created the "obvious potential" to affect the verdict. The Appeals Court, therefore, rejected their claim that the government engaged in improper jury contact.

Prosecutor comments and actions must be taken in context.³⁸ Alleged misconduct that is not flagrant seldom constitutes reversible error.³⁹ Prosecutorial conduct is flagrant if it tends to mislead a jury or prejudice the defendant, if the comments were extensive and not isolated, and if the comments were deliberate. If conduct is not flagrant, this court will not reverse unless "(1) the proof against the defendant was not overwhelming, (2) opposing counsel objected to the conduct, and (3) the district court failed to give a curative instruction."

After thoroughly reviewing the records, the parties' briefs, and the District Court's rulings, the Appeals Court did not find that the District Court abused its discretion. On numerous occasions, the court reminded the jury, in response to the Yangs' objections, that they could consider only the evidence in the record and not what the attorneys said. Even assuming the comments objected to were improper; they were not flagrant and certainly did not prejudice the trial.⁴⁰ The comments at issue here were isolated and inadvertent common usages. Taken in context, with the overwhelming proof of the Yangs' guilt and the court's instruction, the comments do not require a new trial.

The Defendants also moved for a new trial based on newly discovered evidence of Lee's admission in a civil deposition that he had altered a document he had authenticated for the Yangs' criminal trial and that Lee suffered from mental health problems. After his arrest, Lee either began or continued to suffer from mental health problems. He visited a doctor and went to counseling for his difficulty in coping with the change in his circumstances caused by his arrest. As part of his cooperation with the FBI, Lee had given the government all of his files, including his correspondence with the Yangs. Some of the documents Lee gave to the FBI were incomplete because Lee had removed pages that tended to incriminate him. During trial, Lee authenticated some of the incomplete documents that he had given to the government. Later, Lee admitted in a related civil trial that he had excised portions of the letters. The Yangs, however, had copies of the original, unaltered letters from Lee because Lee had mailed those letters to the Yangs years earlier.

The District Court held a hearing on the Yangs' claims and concluded that, as to the changed documents, the evidence withheld by Lee was not newly discovered, since with due diligence the Yangs could have found the originals in their own records; it related to fraud counts on which the Defendants had been acquitted, but was not material to the trade secret counts and was not likely to produce an acquittal. The court further concluded that evidence of Lee's mental problems would not have changed the outcome of the trial, the mental health records contained no exculpatory information, and the absence of the evidence did not affect the fairness or integrity of the trial. The court ruled that the government had committed no *Brady* violation, and that a new trial was not warranted.

The Appeals Court reviewed for abuse of discretion the District Court's denial of a motion for new trial.⁴¹ To prevail on appeal the Yangs had to show that "(1) the new evidence was discovered after the trial; (2) the evidence could not have been discovered earlier with due diligence; (3) the evidence is material and not merely cumulative or impeaching; and (4) the evidence would likely

produce acquittal."⁴² We are satisfied that the District Court did not abuse its discretion. The District Court properly found that the evidence redacted by Lee from the letters, highlighting his criminal involvement, was not material to the Defendants' convictions. Further, the court rightly concluded, in light of the large volume of evidence of guilt and Lee's already largely discredited testimony, that the excised portions of the letters would simply be cumulative and further impeach Lee's credibility. With reference to Lee's medical history, since there was no "reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different," the District Court properly denied the Yangs' motion for a new trial.⁴³

The Defendants raised no objection at the trial to the court's jury instruction on the meaning of "steal." The Appeals Court, therefore, reviewed this claim for plain error.⁴⁴ "An instruction is not plainly erroneous unless there was 'an egregious error, one that directly leads to a miscarriage of justice.'"⁴⁵ The Appeals Court found no plain error. Taken as a whole, the jury instructions fairly and adequately instructed the jury on the issues and the applicable law, and, therefore, if there was any error in this particular instruction, it did not lead to a miscarriage of justice.

Finally, the Defendants asserted that there was insufficient evidence to support their convictions. First, the Defendants claim that the proofs did not establish that the trade secret in question—the Avery patent application—was related to interstate commerce as is required by §1832(a). Second, Sally Yang contends that there was insufficient evidence that she knowingly joined a conspiracy or attempted to steal a trade secret.

The Appeals Court reviewed claims of insufficient evidence to determine whether, taking the evidence in the light most favorable to the prosecution, any reasonable trier of fact could have found the essential elements of the crime beyond a reasonable doubt.⁴⁶ The Appeals Court held that the interstate commerce nexus is sufficiently established in the record. Section 1832(a) requires that the trade

secret in question be “related to or included in a product that is produced for or placed in interstate or foreign commerce.” The patent application given by Lee to the Yangs involved an Avery product generating sales of \$75-100 million the previous year and related to products produced and sold in at least the United States and Canada. Taken as a whole, the testimony was sufficient to permit a reasonable juror to find that Avery is an international company with sales across the world of the product to which the patent application was attached.

Sally’s claim that she was not knowingly involved in a conspiracy cannot withstand the evidence in the record that she had, on numerous occasions, received confidential information from Lee and that she gave Lee payment for his services. A jury could permissibly conclude from this evidence, combined with her actions in the hotel room, that she was knowingly involved in the conspiracy to steal Avery’s trade secrets. The claims of insufficient evidence are without merit.

For all of the reasons set out above, the Appeals Court affirmed the judgments of conviction but vacated the sentence of each of the Defendants and remanded for resentencing.

Endnotes

¹ Rheology is the study of adhesives.

² *United States vs. Alvarez* 266 F.3d 587, 592 (6th Cir. 2001).

³ *Id.* at 192.

⁴ *Id.* at 192-93.

⁵ *Id.* at 193.

⁶ *Hsu*, 155 F.3d at 200-02.

⁷ *Id.* (quoting Model Penal Code § 5.01[1][c] [1985]).

⁸ *id.* at 203 (quoting *United States v. Jannotti*, 673 F.2d 578, 591 [3d Cir. 1982][en banc]).

⁹ *See, e.g., United States v. Mise*, 240 F.3d 527, 530 (6th Cir. 2001); *United States v. Hixon*, 987 F.2d 1261, 1267 (6th Cir. 1993); *United States v. Peete*, 919 F.2d 1168, 1175-76 (6th Cir. 1990).

¹⁰ *See United States v. Barry*, 888 F.2d 1092, 1096-97 (6th Cir. 1990) (internal quotations and citation omitted) (noting that the “cardinal canon of statutory construction” is that statutes “should be interpreted harmoniously with their dominant legislative purpose.”).

¹¹ Model Penal Code §5.01(1)(c). *See also Reeves*, 794 F.2d at 1104 (“In order to prove attempt, the government [must] . . . establish: (1) the intent to engage in criminal activity, and (2) the commission of one or more overt acts . . . towards the commission of the substantive offense.”).

¹² *United States v. Shelton*, 30 F.3d 702, 705 (6th Cir. 1994).

¹³ *United States v. Pearce*, 912 F.2d 159, 161 (6th Cir. 1990) (citation and internal quotations omitted).

¹⁴ *United States v. Hamilton*, 263 F.3d 645, 652 (6th Cir. 2001).

¹⁵ US Sentencing Guidelines Manual (USSG) §5K2.0 (2001).

¹⁶ *Koon v. United States*, 518 U.S. 81, 100 (1996).

¹⁷ *United States v. Coleman*, 188 F.3d 354, 358 (6th Cir. 1999) (en banc).

¹⁸ *United States v. Crouse*, 145 F.3d 786, 789 (6th Cir. 1998).

¹⁹ USSG § 5K2.0.

²⁰ *Koon*, 518 U.S. at 96 (citations omitted).

²¹ 28 U.S.C. § 994(c)-(d).

²² *Koon*, 518 U.S. at 99-100.

²³ *See Burns v. United States*, 501 U.S. 129, 135, n. 4 (1991).

²⁴ *Crouse*, 145 F.3d at 789.

²⁵ *United States v. Guimond*, 116 F.3d 166, 169 (6th Cir. 1997).

²⁶ *United States v. White*, 401 U.S. 745 (1971).

²⁷ *Id.* at 751-52 (“If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that

same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case.”).

²⁸ *Batson v. Kentucky*, 476 U.S. 79 (1986).

²⁹ *United States v. Tucker*, 90 F.3d 1135, 1142 (6th Cir. 1996).

³⁰ *J.E.B. v. Alabama ex rel T.B.*, 511 U.S. 127 (1994); *Batson*, 476 U.S. at 96.

³¹ *Purkett v. Elem*, 514 U.S. 765, 767 (1995) (per curium).

³² *United States v. Sangineto-Miranda*, 859 F.2d 1501, 1520-21 (6th Cir. 1990).

³³ *United States v. DeJongh*, 937 F.2d 1, 3 (1st Cir. 1991) (citing *Geders v. United States*, 425 U.S. 80, 87 (1976)).

³⁴ *See United States v. Malik*, 800 F.2d 143, 149 (7th Cir. 1986) (finding that cross-examination and comment during closing is generally sufficient to dispel any ill effects caused by the coaching).

³⁵ *United States v. Riggsby*, 45 F.3d 120, 125 (6th Cir. 1995).

³⁶ *See Remmer v. United States*, 347 U.S. 227 (1954).

³⁷ *United States v. Frost*, 125 F.3d 346, 377 (6th Cir. 1997).

³⁸ *United States v. Bond*, 22 F.3d 662, 667-68 (6th Cir. 1994).

³⁹ *United States v. Brown*, 66 F.3d 124, 127-28 (6th Cir. 1995).

⁴⁰ *See Bond*, 22 F.3d at 667 (ruling that prosecutor statements do not merit reversal of the District Court unless they permeate the entire trial, making it unfair).

⁴¹ *United States v. Davis*, 15 F.3d 526, 531 (6th Cir. 1994).

⁴² *United States v. Seago*, 930 F.2d 482, 488 (6th Cir. 1991).

⁴³ *Kyles v. Whitley*, 514 U.S. 419, 433-34 (1995) (internal quotations and citation omitted).

⁴⁴ *United States v. King*, 169 F.3d 1035, 1040 (6th Cir. 1999).

⁴⁵ *Id.* (quoting *United States v. Busacca*, 863 F.2d 433, 435 [6th Cir.1988]).

⁴⁶ *United States v. Prince*, 214 F.3d 740, 746 (6th Cir. 2000).

Kelly Therese Warren

Kelly Therese Warren, a former US Army clerk, was sentenced on 12 February 1999 to 25 years in prison on charges that she spied for Hungary and Czechoslovakia while based in Germany during the Cold War. Warren, age 32, from Warner-Robbins, Georgia, was the fourth person convicted and sentenced in Florida for conspiring to commit espionage with Clyde Lee Conrad, a US Army sergeant who gave Hungarian and Czechoslovak agents secret US documents detailing US and NATO plans for the defense of Western Europe.

Warren served from 1984 to 1988 at the US Army's 8th Infantry Division headquarters in Bad Kreuznach in what was then West Germany, where she worked in the G-2 section as an administrative and clerical assistant, preparing classified documents for publication and distribution. The 8th Infantry Division maintained classified US Army, US Air Force, and NATO military documents concerning general defense plans for the allied defense of Europe; plans for the use of tactical nuclear weapons, chemical warfare documents, and coordinating documents used by NATO forces; and technical manuals.

Once Conrad recruited Warren into his ring, she began to either provide documents to him or allowed him to review the documents and files stored in cabinets and distribution boxes located in her office. She also allowed him to remove and photocopy classified information. For example, sometime between the summer 1987 and spring 1988, Warren provided Conrad with a document classified Secret, entitled "Appendix S (CONPLAN LIONHEART ANNEX I [Counterattack Contingency plans] to 8th Inf. Div. [MEC] PLAN 3300 9GDP)."

The espionage ring used the mail, telephone, and a one-way radio link to communicate with each other and with agents and officers of the Hungarian and Czech Intelligence Services. Besides Conrad coming to her office, Warren also passed documents to Conrad in a bowling alley and at a church in Bad Kreuznach.

After reviewing the documents passed by Warren, retired Gen. Clayton Otis, commander of the US Army in Europe from 1983 to 1988, said the papers contained “detailed information regarding how we planned to defend Europe. The compromise of this classified material was devastating to our national security.”¹

Conrad was arrested in 1988 by German authorities and was tried on charges of high treason for espionage on behalf of the Hungarian and Czechoslovak intelligence services between 1976 and 1988. The Koblenz State Appellate Court convicted Conrad on 6 June 1990 and sentenced him to life in prison—the severest sentence handed down in the Federal Republic of Germany for espionage since World War II. Conrad died in a German prison on 8 January 1998.

Besides Warren, the others involved in the espionage ring were Roderick James Ramsey, Stephen Rondeau, and Jeffrey Gregory. They were also convicted in Florida in connection with the conspiracy. Ramsey, arrested in 1990 in Tampa, pleaded guilty and was sentenced in August 1992 to 36 years in prison. Rondeau and Gregory were sentenced in June 1994 to 18 years each.²

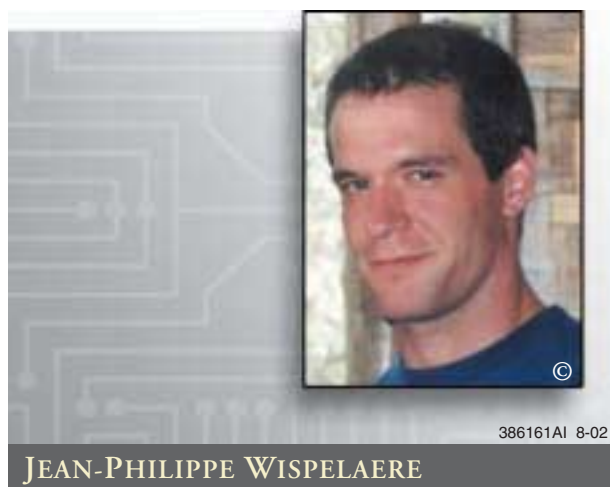
Endnotes

¹ Reuters, “Former U.S. Army Clerk Gets 25 Years in Spy Case,” 19 February 1999.

² See Counterintelligence Reader, Volume Three, “Post-World War II to Closing the 20th Century,” for further information on Conrad (page 257), Gregory (page 409), Ramsey (page 412), and Rondeau (page 413).

Jean-Philippe Wispelaere

Jean-Philippe Wispelaere, a former Australian Government intelligence official, was charged on 17 May 1999 with attempted espionage for selling US defense secrets to an undercover FBI agent posing as a foreign spy. Wispelaere, 28, worked for the Australian Defence Intelligence Organization from July 1998 to January 1999 and held security clearances for access to US top secret and sensitive compartmented information under US-Australian defense treaties.



According to various reports, Wispelaere walked into the embassy of a foreign country in January 1999 in Bangkok, Thailand, and offered to sell classified US documents to that country. The country involved notified US officials, and subsequently, an undercover FBI counterintelligence agent posing as a spy for the foreign country contacted Wispelaere.

Wispelaere corresponded via e-mail with the agent, and in April 1999 he met the man he believed to be a foreign spy in Bangkok and turned over 713 classified US documents in exchange for \$70,000. In early May, Wispelaere mailed more classified documents to the undercover FBI agent at a Virginia post office box in exchange for \$50,000.

On 15 May 1999, Wispelaere flew from London, England, to Dulles International Airport for what

he believed would be a meeting with the foreign spy, but instead, the FBI arrested him upon arrival. After his arrest, he said that he was in “very dire, dire financial need” for a knee operation and “a couple of other concerns, involving females, unfortunately,” the FBI said.

It took nearly two years for the case to come to trial because Wispelaere suffered from a serious spell of schizophrenia and was declared temporarily unable to stand trial in November 1999. Wispelaere said that he was abusing anabolic steroids and using opium and Valium during the period when he stole the documents and tried to sell them. He assured the judge that his five medications now have his illness (hearing voices) under control.

In March 2001, Wispelaere pleaded guilty to attempted espionage. The US Justice Department said that, under a plea agreement, Wispelaere would spend 15 years in jail. Under the plea agreement, Wispelaere is to fully cooperate in debriefings with Australian and US intelligence officials about his activities and to submit to a polygraph test. Prosecutors also agreed to allow Wispelaere to serve five years of his sentence in Australia. He could have faced life in prison.

According to the *Washington Post*, Nina Ginsberg, who represented him, criticized the Australian Government and security service for their lackadaisical attitude toward security vetting. She said the “woefully inadequate vetting process” involved just one face-to-face interview and two phone conversations with people who knew Wispelaere. The Australian spy service apparently did not realize that Wispelaere was using “enormous amounts of steroids” and never questioned him about his travels to more than 100 countries—including several considered terrorist states, Ginsberg said.

Wispelaere took—without any problems—hundreds of spy satellite photos and other classified documents in less than six months with the

Australian spy service. “The things he did, he did under the noses of everyone and no one seemed to notice,” Ginsberg said. “It’s almost comical the mistakes he made. It’s really hard to imagine someone doing a worse job of being a spy.”¹

Endnote

¹ Masters, Brooke, A., “Australian Sentenced for Spying Against the U.S., *The Washington Post*, 8 June 2001.

Mariano Faget

At a February 2000 news conference, the FBI reported that, for more than a year, Mariano Faget, a chief in the Miami office of the US Immigration and Naturalization Service (INS), maintained contacts with Cuban operatives in the United States. According to FBI Special Agent Paul Mallett:



Faget is known to have placed telephone calls to an extension of the Cuban Interests Section, which is a representative office of the Cuban Government in Washington. Faget met with representatives of the Cuban Interests Section. Faget has also had numerous contacts with a Cuban-born resident alien who is the chief executive officer of a business located in New York City, who, in turn, is known to have had several meetings with agents and representatives of the Cuban Government during the past year.

The Cuban-born, 54-year-old Mariano Faget worked for INS for more than 30 years, rising from a low-level clerk to assume a supervisory position in the agency’s hectic Miami field office.

The FBI became suspicious of Faget after they spotted him meeting with a Cuban Interests Section official at a Miami airport bar more than a year ago. After months of surveillance, the FBI and INS launched a sting operation codenamed “False Blue.” On 11 February 2000, FBI Special Agent in Charge Hector Pesquera appeared at Faget’s

office requesting help in preparing immigration documents in a “highly sensitive” and top-secret Cuban defection.

Pesquera identified the defector as Luis Molina, one of two “known Cuban intelligence officers” seen meeting alone with Faget at two different Miami nightspots during 1999. “Let me tell you something,” Faget told Pesquera. “I don’t know if this is going to make a difference, I’ve met this guy before. . . . He was at the Interests Section in Cuba, in Washington, D.C., and I went to a dinner here one day and he happened to be there.” When Pesquera asked, “That’s it? That’s your only contact with him?” Faget responded, “That’s the only contact.”

INS agents told Mariano Faget that they needed him to process asylum papers for a Cuban intelligence officer who was supposedly about to defect. Special Agent Mallett described what allegedly happened next:

Faget was told that the information he was being entrusted with was secret and very sensitive. The meeting was both videotaped and audiotaped. Approximately twelve minutes after that meeting, Faget placed a telephone call from his office to the offices of the New York businessman. Faget identified the full name of the individual for whom he had been asked to prepare the political asylum document.

Faget’s call was to his longtime friend and America Cuba Incorporated (ACI) partner, Pedro Font. At the time, Faget was secretary and vice president for ACI, which was formed in 1993 to act as a conduit for American retailers looking to enter Cuba after the fall of Fidel Castro’s communist regime. Font was set to meet on 11 February 2000 with Jose Imperatori, another Cuban Interests Section official they both knew.

At his trial, Faget argued that the lie to Pesquera was immaterial, that he voluntarily disclosed the relationship, and that ACI is a Florida corporation that had done no business at all in the United States—let alone in a foreign country. Faget

claimed his motive was to warn Font to be wary, not so Font could pass along the secret. Prosecutors maintained Faget intended the secret to curry favor with Font and, in turn, Cuban officials.

The FBI also said Faget was guilty of making false statements to federal officials. Faget admitted at his trial that he lied to the FBI and that he disclosed classified information without permission—two factors that formed the foundation for the government’s case. Faget said he did it to protect a lifelong friend and business partner. Prosecutors said he did it for greed and to court favor with Cuban officials he viewed as prospective business contacts. According to prosecutors, that was the first in a long succession of lies told by Faget. Another alleged lie came in May 1998 when he denied any “foreign business contacts” on his reapplication for a security clearance.

The US District Attorney for Miami, Tom Scott, said other suspects could also be charged. “Are we going to charge Cuban agents in Washington? It’s an ongoing investigation, but I think you can anticipate further action and announcements.”

Two weeks later, Faget spoke with a Miami television station from the detention center where he had been held since 17 February. The Cuban-born suspect, who came to the United States as a young man, said he never passed sensitive information to any foreign agents. “I am a moral person. I love this country and I would never do anything to hurt it. And what would I have to gain by giving information? There’s nothing to gain there. I’ve never considered doing anything like that.”

Faget acknowledged he contacted the New York businessman, but insists his intention was not to betray the supposed Cuban defector. He also admits that, in late 1998, he met with Cuban diplomat Imperatori, whom the United States has also expelled from the country for spying. Faget said he was never asked, nor did he volunteer, any US secrets. “That meeting was the first time I met him. We discussed, in general, the future of Cuba. My job never entered into (had any part of) any

conversations with him.” Faget was denied bail while awaiting trial and said he is eager to have his day in court.

On 24 February, Miami Federal Magistrate Judge Barry Garber denied bail for Faget saying there was a risk he might flee if released from jail. In court, Faget expressed a desire to clear his name, stating he has never sympathized with communism.

During the trial, prosecutors used the surveillance tapes to prove their case, while Faget’s lawyer challenged the charge—required for a conviction—that Faget intended to harm the United States or help Cuba. “Mariano Faget was a government employee willing to betray the trust of people he was sworn to serve,” Assistant U.S. Attorney Curtis Miner told the jurors. “He disclosed classified information for no better purpose than his own personal reasons, his own personal gain.” Faget’s defense attorney, Edward O’Donnell, called Faget “an honest government servant who made a mistake.” Faget was close to retirement after 34 years with the INS.

It was also learned during the trial that the FBI tried to recruit Faget as an agent working for the United States before arresting him. The FBI wanted to find out all they could about his links to Cuban intelligence, said FBI agent James Laflin. “We did not achieve either objective, because Mr. Faget was manipulative and deceitful,” said Laflin. “It was clear there was no way we could use him” in the future as a counterintelligence agent. “We told him at the end that that was his final chance to tell the truth. We had no choice but to put him under arrest.”

On 30 May 2000, a jury found Faget guilty on four counts of violating the Espionage Act by disclosing official secrets and lying about his contact with Cuban diplomats. He had been in prison without bail since his arrest and remained in custody after the verdict. Federal sentencing guidelines call for a sentence of 62 to 75 months.

The case further strained the thorny relations between Washington and Havana when, three days

after Faget’s arrest, the State Department ordered the expulsion of Washington-based Cuban consular official Jose Imperatori, one of two Cuban officials Faget was known to have met. Imperatori had accompanied Elian Gonzalez’s grandmothers from Washington to Miami on the first of their two visits here, but prosecutors made no links between Faget and the case of the Cuban boy. Cuba has ordered the diplomat to remain in the United States and challenge accusations of espionage.

The US State Department said Imperatori was expelled from the United States for not voluntarily leaving the country by the deadline of midday 26 February 2000. The 46-year-old diplomat, who had worked at the Cuban Interests Section in Washington, was not handcuffed and looked impassive as federal agents took him to Reagan National Airport outside Washington for a government flight to Montreal. A Canadian commercial flight was to take him back to Cuba.

At a 26 February 2000 news conference, Imperatori strongly denied links to Faget. At a separate news conference the same day, Cuban Interests Section spokesman Fernando Ramirez acknowledged his colleague had had contacts with Faget but insisted they were not criminal in nature. “We want to be very clear that he is completely innocent, that he didn’t do anything wrong, that the Cuban Interests Section in Washington does not do any kind of intelligence or espionage activities.”

Ramirez insisted there was a link between Faget’s arrest and the custody battle over six-year-old Gonzalez, a shipwreck victim saved off the US coast and that Havana demanded he be returned to his father in Cuba. Court papers identified Imperatori as the immigration official’s Washington contact.

Imperatori earlier had resigned his post as Consular Affairs Officer, leaving him without diplomatic immunity and insisting he is a victim of what he called a major slander. His refusal to leave voluntarily came as no surprise as Cuban officials signaled they had no intention of willingly abiding by the deportation order.

In a statement issued on 22 February 2000 by Cuba's ruling Communist party, the Castro government accused the United States of operating a large spying operation out of its seven-story Interests Section building on the Havana waterfront. The Cuban statement alleged that the building is full of sophisticated listening devices and electronic spying equipment. It also said that most of the people working there are CIA agents, who the Castro government claims work closely with so-called "mercenaries"—a reference to political dissidents and independent journalists within Cuba. There are so many spies in the US Interests Section, according to the communique, that if Cuba asked them all to leave—in the words of the statement—"there would be few or none left."

As for the US allegations against Imperatori, the statement challenged the United States to present the charges in court. The Cuban Government denied ever having used its Interests Section in Washington for espionage. The Castro government claimed the US allegations against Imperatori were designed to undermine the case for returning Gonzalez to his father in Cuba. The statement noted the timing of the accusation, coming just before the federal hearing on the case in Miami.

On 29 June 2001, US District Judge Alan Gold sentenced Faget to five years in prison for disclosing classified information to Cuba. Because US Attorney Guy Lewis said that Faget's disclosure caused "no overt harm to the national security," Judge Gold rejected guidelines calling for a term of 10 years.

Echelon

The allegations of U.S. industrial espionage have provoked calls for the European Union to set up a committee of inquiry to look into the issue. The demand emerged as a European Union parliamentary committee studied a report by British Journalist Duncan Campbell. Mr. Campbell's report claims the United States, Britain and other key allies have, since the cold war, maintained a sophisticated electronic spy network called "Echelon."

European-Union member Britain helps operate the system, along with listening posts in Canada, Australia, and New Zealand. A British news report says the system led by the US National Security Agency has engaged in industrial espionage against European businesses.

Campbell's report says the network of spy satellites and electronic eavesdropping equipment can monitor phone conversations, faxes, and electronic mail. The report calls the surveillance network a threat to civil liberties and alleges it has been used to collect economically sensitive information that provides a commercial advantage to U-S companies.

Green Party members of the European Parliament demanded a committee of inquiry look into the charges based on Campbell's and other reports on Echelon's monitoring capabilities. They also say information gathered by Echelon helped the United States beat the European Airbus Consortium in selling aircraft to Saudi Arabia in 1994.

According to the British report, the Echelon program monitors worldwide communications with a network of satellite and ground based listening posts. The network was established during the cold war for military surveillance. French officials have alleged that Britain has also benefited commercially from information gathered by the network, allegations British Prime Minister Tony Blair has denied.¹

The European Commission has a problem in investigating these damages. Commission spokesman Jonathan Faull explains that no European business has complained about damages from spying. “Nobody has come forward, and we should certainly be interested in talking to people who want to come forward, but nobody has done so.”

Another problem is that Britain is a member of the European Union. In a letter released by the Commission, the British government cites 1985 legislation that authorizes interception of communications in cases involving safeguarding the nation’s economic well being.

The Commission also has a letter from the State Department stating that the US intelligence community is not engaged in industrial espionage. The letter also says the US Government does not collect information for the benefit of private firms.

Likewise, State Department spokesman James Rubin refused to comment on the existence of the system, but he denied US intelligence agencies are engaged in industrial espionage. “US intelligence agencies are not tasked to engage in industrial espionage, or obtain trade secrets for the benefit of any US company or companies.”

The European Commission has been aggravated by interviews given by the former director of the CIA James Woolsey. He justified industrial espionage by the United States on the basis of the use of bribery by European companies.

Commission spokesman Faull expresses outrage about the justification, while not denying bribery is sometimes used to make a sale. “I do not deny that cases of bribery arise in all sorts of countries by the way, not only in Europe, from time to time, I am not that naive. What I am saying is outrageous is the suggestion is that espionage could be justified in order to redress some apparent imbalance caused by the fact that European companies are considered to bribe more than American companies.”

In the European Parliament’s debate, Portuguese Interior Minister Fernando Gomes says the EU

justice ministers would discuss the Echelon system in their meeting at the end of April. He said the European Union couldn’t accept the existence of such a system that violates data privacy. But he also said there is no evidence that companies ever benefited from communications interception or have been damaged by it.²

The following is an edited version of the European Parliament’s report on ECHELON.

On 5 July 2000 the European Parliament decided to create a temporary committee to investigate the ECHELON system. This step was prompted by the debate on the study commissioned by STOA³ [Scientific and Technical Options Assessment Program, Office of the European Parliament] concerning the so-called ECHELON system,⁴ which the author, Duncan Campbell, had presented at a hearing of the Committee on Citizens Freedoms and Rights, Justice and Home Affairs on the subject, the European Union and data protection.

The first STOA report of 1997, which STOA commissioned from the Omega Foundation for the European Parliament in 1997, on *An Appraisal of Technologies of Political Control* described ECHELON in a chapter concerning national and international communications interception networks. The author claimed that all e-mail, the US National Security Agency routinely intercepted telephone and fax communications in Europe.⁵ As a result of this report, the alleged existence of a comprehensive global interception system called ECHELON was brought to the attention of people throughout Europe.

In 1999, in order to find out more about this subject, STOA commissioned a five-part study of the development of surveillance technology and risk of abuse of economic information. Part 2/5, by Duncan Campbell, concerned the existing intelligence capacities and particularly the mode of operation of ECHELON.⁶

Concern was aroused in particular by the assertion in the report that ECHELON had moved away

from its original purpose of defense against the Eastern Bloc and was currently being used for purposes of industrial espionage. Examples of alleged industrial espionage were given in support of the claim: in particular, it was stated that Airbus and Thomson CFS had been damaged as a result. Campbell bases his claims on reports in the American press.⁷ As a result of the STOA study, ECHELON was debated in the parliaments of virtually all the Member States; in France and Belgium, reports were even drafted on it.

At the same time as it decided to set up a temporary committee, the European Parliament drew up its mandate.⁸ It reads as follows:

- to verify the existence of the communications interception system known as ECHELON, whose operation is described in the STOA report published under the title Development of surveillance technology and risks of abuse of economic information;
- to assess the compatibility of such a system with Community law, in particular Article 286 of the EC Treaty and Directives 95/46/EC and 97/66/EC, and with Article 6(2) of the EU Treaty, in the light of the following questions:
 - Are the rights of European citizens protected against activities of secret services?
 - Is encryption an adequate and sufficient protection to guarantee citizens privacy or should additional measures be taken and if so what kind of measures?
 - How can the EU institutions be made better aware of the risks posed by these activities and what measures can be taken?
 - To ascertain whether European industry is put at risk by the global interception of communications;
 - Possibly, to make proposals for political and legislative initiatives.

The European Parliament decided to set up a temporary committee because a committee of inquiry can be set up only to investigate violations of Community law under the EC Treaty (Article 193 TEC [Truth About Europe Campaign]), and

such committees can accordingly only consider matters governed by it. Matters falling under Titles V (Common Foreign and Security Policy) and VI (Police and Judicial Cooperation in Criminal Matters) of the Treaty on European Union are excluded. Moreover, under the inter-institutional decision⁹ the special powers of a committee of inquiry to call people to appear and to inspect documents apply only if grounds of secrecy or public or national security do not dictate otherwise, which would certainly make it impossible to summon secret services to appear. Furthermore, a committee of inquiry cannot extend its work to third countries, because by definition the latter cannot violate EU law. Thus, setting up a committee of inquiry would only have restricted the scope of any investigations opening up any additional rights, for which reason the idea was rejected by a majority of Members of the European Parliament.

With a view to carrying out its mandate in full, the committee decided to proceed in the following way. A program of proposed work adopted by the committee listed the following relevant topics: certain knowledge about ECHELON; debate by national parliaments and governments; intelligence services and their operations; communications systems and the scope for intercepting them; encryption; industrial espionage; aims of espionage and protective measures; legal context and protection of privacy; and implications for the EU's external relations.

The topics were considered consecutively at the individual meetings, the order of consideration being based on practical grounds and thus not implying anything about the value assigned to the individual topics. At the meetings, in accordance with the requirements of the topic concerned, representatives of national administrations (particularly secret services) and parliaments in their capacity as bodies responsible for monitoring secret services were invited to attend. Also attending were legal experts and experts in the fields of communications and interception technology, business security and encryption technology with both academic and practical

backgrounds. Journalists who had investigated this field were also heard.

The meetings were generally held in public, although some sessions were also held behind closed doors where this was felt to be advisable in the interests of obtaining information. In addition, the chairman of the committee and the reporter visited London and Paris together to meet people who for a wide variety of different reasons were unable to attend meetings of the committee but whose involvement in the committee's work nonetheless seemed advisable. For the same reasons, the committee's bureau, the coordinators and the reporter traveled to the USA. The reporter also held many one-to-one talks, in some cases in confidence.

The system known, as ECHELON is an interception system, which differs from other intelligence systems in that it possesses two features, which make it quite unusual. The first such feature attributed to it is the capacity to carry out quasi-total surveillance. Satellite receiver stations and spy satellites in particular are alleged to give it the ability to intercept any telephone, fax, Internet or e-mail message sent by any individual and thus to inspect its contents.

The second unusual feature of ECHELON is that the system operates worldwide on the basis of cooperation proportionate to their capabilities among several states (the UK, the USA, Canada, Australia and New Zealand), giving it an added value in comparison to national systems. The states participating in ECHELON can place their interception systems at each other's disposal, share the cost and make joint use of the resulting information.

This type of international cooperation is essential in particular for the worldwide interception of satellite communications, since only in this way is it possible to ensure in international communications that both sides of a dialogue can be intercepted. It is clear that, in view of its size, a satellite receiver station cannot be established on the territory of a state without that state's knowledge. Mutual agreement and proportionate cooperation among several states in different parts of the world is essential.

Possible threats to privacy and to businesses posed by a system of the ECHELON type arise not only from the fact that is a particularly powerful monitoring system, but also that it operates in a largely legislation-free area. Systems for the interception of international communications are not usually targeted at residents of the home country. The person whose messages were intercepted would have no domestic legal protection, not being resident in the country concerned. Such a person would be completely at the mercy of the system.

Parliamentary supervision would also be inadequate in this area, since the voters, who assume that interception only affects people abroad, would not be particularly interested in it, and elected representatives chiefly follow the interests of their voters. That being so, it is hardly surprising that the hearings held in the US Congress concerning the activities of the NSA were confined to the question of whether US citizens were affected by it, with no real concern expressed regarding the existence of such a system in itself. It thus seems all the more important to investigate this issue at European level.

The Operations of Foreign Intelligence Services

In addition to police forces, most governments run intelligence services to protect their country's security. As their operations are generally secret, they are also referred to as secret services. These services have the following tasks: gathering information to avert dangers to state security; counter-espionage in general; averting possible dangers to the armed forces; and gathering information about situations abroad.

Governments have a need for systematic collection and evaluation of information about certain situations in other states. This serves as a basis for decisions concerning the armed forces, foreign policy and so on. They therefore maintain foreign intelligence services, part of whose task is to systematically assess information available from public sources. The reporter has been informed

that on average this accounts for at least 80% of the work of the intelligence services.¹⁰ However, particularly significant information in the fields concerned is kept secret from governments or businesses and is therefore not publicly accessible. Anyone who nonetheless wishes to obtain it has to steal it. Espionage is simply the organized theft of information.

The classic targets of espionage are military secrets, other government secrets or information concerning the stability of or dangers to governments. These may for example comprise new weapons systems, military strategies or information about the stationing of troops. No less important is information about forthcoming decisions in the fields of foreign policy, monetary decisions or inside information about tensions within a government. In addition there is also interest in economically significant information. This may include not only information about sectors of the economy but also details of new technologies or foreign transactions.

Espionage involves gaining access to information, which the holder would rather protect from being accessed by outsiders. This means that the protection needs to be overcome and penetrated. This is the case with both political and industrial espionage. Thus the same problems arise with espionage in both fields, and the same techniques are accordingly used in both of them. Logically speaking there is no difference, only the level of protection is generally lower in the economic sphere, which sometimes makes it easier to carry out industrial espionage. In particular, businessmen tend to be less aware of risks when using interceptible communication media than does the state when employing them in fields where security is a concern.

Protection of secret information is always organized in the same way:

- Only a small number of people, who have been vetted, have access to secret information;
- There are established rules for dealing with such information;

- Normally the information does not leave the protected area, and if it does so, it leaves only in a secure manner or encrypted form. The prime method of carrying out organized espionage is therefore by gaining access to the desired information directly through people (human intelligence). These may be:

1. Plants (agents) acting on behalf of the service/business engaging in espionage;
2. People recruited from the target area.

Recruits generally work for an outside service or business for the following reasons:

- Sexual seduction;
- Bribery in cash or in kind;
- Blackmail;
- Ideological grounds;
- Attachment of special significance or honor to a given action (playing on dissatisfaction or feelings of inferiority).

A borderline case is unintentional cooperation by means of which information is creamed off. This involves persuading employees of authorities or businesses to disclose information in casual conversation, for example by exploiting their vanity, under apparently harmless circumstances (through informal contact at conferences or trade fairs or in hotel bars).

The use of people has the advantage of affording direct access to the desired information. However, there are also disadvantages:

- Counter-espionage always concentrates on people or controlling agents;
- Where an organization's staff are recruited, the weaknesses which laid them open to recruitment may rebound on the recruiting body;
- People always make mistakes, which means that sooner or later they will be detected through counterespionage operations.

Where possible, therefore, organizations try to replace the use of agents or recruits with non-human espionage. This is easiest in the case

of the analysis of radio signals from military establishments or vehicles.

The form of espionage by technical means with which the public is most familiar is that which uses satellite photography. In addition, however, electromagnetic signals of any kind are intercepted and analyzed (Signals Intelligence-SIGINT).

In the military field, certain electromagnetic signals, e.g. those from radar stations, may provide valuable information about the organization of enemy air defenses (electronic intelligence-ELINT). In addition, electromagnetic radiation, which could reveal details of the position of troops, aircraft, ships or submarines, is a valuable source of information for an intelligence service. Monitoring other states spy satellites, which take photographs, and recording and decoding signals from such satellites, is also useful.

Ground stations record the signals from low-orbit satellites or from quasi-geostationary SIGINT satellites. This aspect of intelligence operations using electromagnetic means consumes a large part of services' interception capacity. However, this is not the only use made of technology.

The foreign intelligence services of many states intercept the military and diplomatic communications of other states. Many of these services also monitor the civil communications of other states if they have access to them. In some states, services are also authorized to monitor incoming or outgoing communications in their own country. In democracies, intelligence services monitoring of the communications of the country's own citizens is subject to certain triggering conditions and controls. However, domestic law in general only protects nationals within the territory of their own country and other residents of the country concerned

The Operations of Certain Intelligence Services

Public debate has been sparked primarily by the interception operations of the US and British intelligence services. They have been criticized for recording and analyzing communications (voice, fax, E-mail). A political assessment requires a yardstick for judging such operations. The interception operations of foreign intelligence services in the EU may be taken as a basis for comparison. Table 1 provides an overview. It shows that interception of private communications by foreign intelligence services is by no means confined to the US or British foreign intelligence services.

Country	Communications in foreign countries	State communications	Civilian communications
Belgium	+	+	+
Denmark	+	+	+
Finland	+	+	+
France	+	+	+
Germany	+	+	+
Greece	+	+	-
Ireland	-	-	-
Italy	+	+	+
Luxembourg	-	-	-
Netherlands	+	+	+
Austria	+	+	-
Portugal	+	+	-
Sweden	+	+	+
Spain	+	+	+
UK	+	+	+
USA	+	+	+
Canada	+	+	+
Australia	+	+	+
New Zealand	+	+	+

Table 1: Interception operations by intelligence services in the EU and in the UKUSA states.¹¹

Technical Conditions Governing the Interception of Telecommunications

If people wish to communicate with one another over a given distance, they need a medium. This medium may be air (sound waves); light (Morse lamp, fiber optic cable); electric current (telegraph, telephone); or an electromagnetic wave (all forms of radio). Any third party who succeeds in accessing the medium can intercept the communications. This process may be easy or difficult, feasible anywhere or only from certain locations. Two extreme cases are discussed below—the technical possibilities available to a spy working on the spot, on the one hand, and the scope for a worldwide interception system, on the other.

On the spot, any form of communication can be intercepted if the eavesdropper is prepared to break the law and the target does not take protective measures. Conversations in rooms can be intercepted by means of planted microphones (bugs) or laser equipment which picks up vibrations in windowpanes. Screens emit radiation, which can be picked up at a distance of up to 30 meters, revealing the information on the screen.

Telephone, fax, and e-mail messages can be intercepted if the eavesdropper taps into a cable leaving the relevant building. Although the infrastructure required is costly and complex, communications from a mobile phone can be intercepted if the interception station is situated in the same radio cell (diameter 300-m in urban areas, 30 km in the countryside).

Closed-circuit communications can be intercepted within the USW-radio range. Conditions for the use of espionage equipment are ideal on the spot, since the interception measures can be focused on one person or one target and almost every communication can be intercepted. The only disadvantage may be the risk of detection in connection with the planting of bugs or the tapping of cables.

Today, various media are available for all forms of intercontinental communication (voice, fax and data). The scope for a worldwide interception system is restricted by two factors: restricted access to the communication medium and the need to filter out the relevant communication from a huge mass of communications taking place at the same time.

All forms of communication (voice, fax, e-mail, and data) are transmitted by cable. Access to the cable is a prerequisite for the interception of communications of this kind. Access is certainly possible if the terminal of a cable connection is situated on the territory of a state, which allows interception. In technical terms, therefore, within an individual state all communications carried by cable can be intercepted, provided this is permissible under the law. However, foreign intelligence services generally have no legal access to cables situated on the territory of other states. At best, they can gain illegal access to a specific cable, although the risk of detection is high.

From the telegraph age onwards, intercontinental cable connections have been achieved by means of underwater cables. Access to these cables is always possible at those points where they emerge from the water. If several states join forces to intercept communications, access is possible to all the terminals of the cable connections situated in those states. This was historically significant, since both the underwater telegraph cables and the first underwater coaxial telephone cables linking Europe and America landed in Newfoundland and the connections to Asia ran via Australia, because regenerators were required.

Today, fiber optic cables follow the direct route, regardless of the mountainous nature of the ocean bed and the need for regenerators, and do not pass via Australia or New Zealand. Electric cables may also be tapped between the terminals of a connection, by means of induction (i.e. Electro-magnetically, by attaching a coil to the cable), without creating a direct, conductive connection. Underwater electric cables can also be tapped in this way from submarines, albeit at very high cost. This technique was employed by the USA in order

to tap into a particular underwater cable laid by the USSR to transmit unencrypted commands to Soviet atomic submarines. The high costs alone rule out the comprehensive use of this technique.

In the case of the older-generation fiber optic cables used today, inductive tapping is only possible at the regenerators. These regenerators transform the optical signal into an electrical signal, strengthen it and then transform it back into an optical signal. However, this raises the issue of how the enormous volumes of data carried on a cable of this kind can be transmitted from the point of interception to the point of evaluation without the laying of a separate fiber optic cable.

On cost grounds, the use of a submarine fitted with processing equipment is conceivable only in very rare cases, for example in wartime, with a view to intercepting the enemy's strategic military communications. The use of submarines for the routine surveillance of international telephone traffic can be ruled out.

The new-generation fiber optic cables use erbium lasers as regenerators. Interception by means of electromagnetic coupling is thus no longer possible. Communications transmitted using fiber optic cables of this kind can thus only be intercepted at the terminals of the connection.

The practical implication for the UKUSA states is that communications can be intercepted at acceptable cost only at the terminals of the underwater cables, which land on their territory. Essentially, therefore, they can only tap incoming or outgoing cable communications. In other words, their access to cable communications in Europe is restricted to the territory of the United Kingdom, since hitherto internal communications have mostly been transmitted via the domestic cable network. The privatization of telecommunications may give rise to exceptions, but these are specific and unpredictable.

This is valid at least for telephone and fax communications. Other conditions apply to

communications transmitted over the Internet via cable. The situation can be summarized as follows:

- Internet communications are carried out using data packets and different packets addressed to the same recipient may take different routes through the network.
- At the start of the Internet age, spare capacity in the public network was used for the transmission of e-mail communications. For that reason, the routes followed by individual data packets were completely unpredictable and arbitrary. At that time, the most important international connection was the science backbone between Europe and America.
- The commercialization of the Internet and the establishment of Internet providers also resulted in a commercialization of the network. Internet providers operated or rented their own networks. They therefore made increasing efforts to keep communications within their own network in order to avoid paying user fees to other operators. Today, the route taken through the network by a data packet is therefore not solely determined by the capacity available on the network, but also hinges on cost considerations.
- An E-mail sent from a client of one provider to a client of another provider is generally routed through the firm's network, even if this is not the quickest route. Routers, computers situated at network junctions and which determine the route by which data packets will be transmitted, organize the transition to other networks at points known as switches.
- At the time of the science backbone, the switches for the routing of global Internet communications were situated in the USA. For that reason, at that time intelligence services could intercept a substantial proportion of European Internet communications. Today, only a small proportion of intra-European Internet communications is routed via the USA.¹²
- A small proportion of intra-European communications is routed via a switch in London to which, since foreign communications are involved, the British monitoring station GCHQ has access. The majority of communications do not leave the continent:

for example, more than 95% of intra-German Internet communications are routed via a switch in Frankfurt.

In practical terms, this means that the UKUSA states have access only to a very limited proportion of Internet communications transmitted by cable.

The interceptibility of radio communications depends on the range of the electromagnetic waves employed. If the radio waves run along the surface of the earth (so-called ground waves), their range is restricted and is determined by the topography of the earth's surface, the degree to which it is built up and the amount of vegetation. If the radio waves are transmitted towards space (so-called space waves), two points a substantial distance apart can be linked by means of the reflection of the sky wave from layers of the ionosphere. Multiple reflections substantially increase the range.

The range is determined by the wavelength:

- Very long and long waves (3 kHz \ominus 300 kHz) propagate only via ground waves, because space waves are not reflected. They have very short ranges.
- Medium waves (300 kHz \ominus 3 MHz) propagate via ground waves and at night also via space waves. They are medium-range radio waves.
- Short waves (3 MHz \ominus 30 MHz) propagate primarily via ground waves; multiple reflections make worldwide reception possible.
- Ultra-short waves (30 MHz \ominus 300 MHz) propagate only via ground waves, because space waves are not reflected. They propagate in a relatively straight line, like light, with the result that, because of the curvature of the earth, their range is determined by the height of the transmitting and receiving antennae. Depending on power, they have ranges of up to 100 km (roughly 30 km in the case of mobile phones).
- Decimeter and centimeter waves (30 MHz \ominus 30 GHz) propagate in a manner even more akin to light than ultra-short waves. They are easy to focus, clearing the way for low-power, unidirectional transmissions (ground-based

microwave radio links). They can only be received by antennae situated almost or exactly in line-of-sight.

Long and medium waves are used only for radio transmitters, radio beacons, etc. Short wave and above all, USW and decimeter/centimeter waves are used for military and civil radio communications.

The details outlined above show that a global communications interception system could only intercept short-wave radio transmissions. In the case of all other types of radio transmission, the interception station must be situated within a 100-km radius (e.g. on a ship, in an embassy). The practical implication for the UKUSA states with terrestrial listening stations is that they can intercept only a very limited proportion of radio communications.

As already referred to above, decimeter and centimeter waves can very easily be focused to form microwave radio links. If a microwave radio link is set up transmitting to a telecommunications satellite in a high, geostationary orbit and the satellite receives the microwave signals, converts them and transmits them back to earth, large distances can be covered without the use of cables. The range of such a link is essentially restricted only by the fact that the satellite can receive and transmit only in a straight line. For that reason, several satellites are employed to provide worldwide coverage. If UKUSA States operate listening stations in the relevant regions of the earth, in principle they can intercept all telephone, fax and data traffic transmitted via such satellites.

It has long been known that special AWACS aircraft are used for the purpose of locating other aircraft over long distances. The radar equipment in these aircraft works in conjunction with a detection system designed to identify specific objectives, which can locate forms of electronic radiation, classify them and correlate them with radar sightings. They have no separate SIGINT capability.¹³ In contrast, the slow flying EP-3 spy

plane used by the US Navy has the capability to intercept microwave, USW and short-wave transmissions. The signals are analyzed directly on board and the aircraft is used solely for military purposes.¹⁴ In addition, surface ships, and in coastal regions, submarines are used to intercept military radio transmissions.¹⁵

Provided they are not focused through the use of appropriate antennae, radio waves radiate in all directions, i.e. also into space. Low-orbit Signals Intelligence Satellites can only lock on to the target transmitter for a few minutes in each orbit. In densely populated, highly industrialized areas interception is hampered to such a degree by the high density of transmitters using similar frequencies that it is virtually impossible to filter out individual signals.¹⁶ The satellites cannot be used for the continuous monitoring of civilian radio communications.

Alongside these satellites, the USA operates so-called quasi-geostationary SIGINT satellites stationed in a high earth orbit (42 000 km).¹⁷ Unlike the geostationary telecommunications satellites, these satellites have an inclination of between 3 and 10°, an apogee of between 39,000 and 42,000 km, and a perigee of between 30,000 and 33,000 km. The satellites are thus not motionless in orbit, but move in a complex elliptical orbit, which enables them to cover a larger area of the earth in the course of one day and to locate sources of radio transmissions. This fact, and the other non-classified characteristics of the satellites, points to their use for purely military purposes. The signals received are transmitted to the receiving station by means of a strongly-focused, 24 GHz downlink.

When foreign communications are intercepted, no single telephone connection is monitored on a targeted basis. Instead, some or all of the communications transmitted via the satellite or cable in question are tapped and filtered by computers employing keywords—analysis of every single communication would be completely impossible.

It is easy to filter communications transmitted along a given connection. Specific faxes and e-mails can also be singled out through the use of keywords. If the system has been trained to recognize a particular voice, communications involving that voice can be singled out. However, the automatic recognition to a sufficient degree of accuracy of words spoken by any voice is not yet possible. Moreover, the scope for filtering out is restricted by other factors: the ultimate capacity of the computers, the language problem and, above all, the limited number of analysts who can read and assess filtered messages.

When assessing the capabilities of filter systems, consideration must also be given to the fact that in the case of an interception system working on the basis of the vacuum-cleaner principle, those technical capabilities are spread across a range of topics. Some of the keywords relate to military security, some to drug trafficking and other forms of international crime, some to the trade in dual-use goods and some to compliance with embargoes. Some of the keywords also relate to economic activities. Any move to narrow down the range of keywords to economically interesting areas would simply run counter to the demands made on intelligence services by governments; what is more, even the end of the Cold War was not enough to prompt such a step.

The Example of the German Federal Intelligence Service

Department 2 of the German Federal Intelligence Service (FIS) obtains information through the interception of foreign communications. This activity was the subject of a review by the German Federal Constitutional Court. The details made public during the court proceedings combined with the evidence given to the Temporary Committee on 21 November 2000 by Mr. Ernst Uhrlau, the coordinator for the secret services in the Federal Chancellor's Office, give an insight into the scope for obtaining intelligence by intercepting satellite communications.¹⁸

On the basis of differing legal provisions or the availability of a greater number of analysts, the capabilities of other intelligence services may be greater in detail terms in given areas. In particular, the monitoring of cable traffic increases the statistical likelihood of success, but not necessarily the number of communications, which can be analyzed. In fundamental terms, the example of the FIS demonstrates the capabilities and strategies employed by foreign intelligence services in connection with the monitoring of foreign communications, even if those services do not disclose such matters to the public.

The FIS endeavors, by means of strategic telecommunications monitoring, to secure information from foreign countries about foreign countries. With that aim in view, satellite transmissions are intercepted using a series of search terms (which in Germany must be authorized in advance by the so-called G10 Committee¹⁹). The relevant figures break down as follows (year 2000): of the roughly 10 million international communications routed to and from Germany every day, some 800 000 are transmitted via satellite. Just under 10% of these (75 000) are filtered through a search engine.

This limitation is not imposed by the law (in theoretical terms, and at least prior to the proceedings before the Federal Constitutional Court, a figure of 100% would have been allowable), but derives from technical restrictions, e.g. the limited capacity for analysis. The number of usable search terms is likewise restricted on technical grounds and by the need to secure authorization.

The grounds for the judgment handed down by the Federal Constitutional Court refer, alongside the purely formal search terms (connections used by foreign nationals or foreign firms abroad), to 2,000 search terms in the sphere of nuclear proliferation, 1,000 in the sphere of the arms trade, 500 in the sphere of terrorism and 400 in the sphere of drug trafficking. However, the procedure has proved relatively unsuccessful in connection with terrorism and drug trafficking.

The search engine checks whether authorized search terms are used in fax and telex communications. Automatic word recognition in voice connections is not yet possible. If the search terms are not found, in technical terms the communications automatically end up in the waste bin; they cannot be analyzed, owing to the lack of a legal basis. Every day, five or so communications are logged, which are covered by the provisions governing the protection of the German constitution. The monitoring strategy of the FIS is geared to finding clues on which to base further monitoring activities. The monitoring of all foreign communications is not an objective. This also applies to the SIGINT activities of other foreign intelligence services.

Satellite Communications Technology

Today, telecommunications satellites form an essential part of the global telecommunications network and have a vital role to play in the provision of television and radio programs and multimedia services. Nevertheless, the proportion of international communications accounted for by satellite links has decreased substantially over the past few years in Central Europe; it lies between 0.4 and 5%.²⁰ This can be explained by the advantages offered by fiber optic cables, which can carry a much greater volume of traffic at a higher connection quality.

Today, voice communications are also carried by digital systems. The capacity of digital connections routed via satellites is restricted to 1,890 ISDN-standard [Integrated Services Digital Network] (64 kbits/sec) voice channels per transponder on the satellite in question. In contrast, 241,920 voice channels with the same standard can be carried on a single optical fiber. This corresponds to a ratio of 1:128.

In addition, the quality of connections routed via satellite is lower than those routed via underwater fiber optic cables. In the case of normal voice transmissions, the loss of quality resulting from the long delay times of several hundred milliseconds is hardly noticeable—although it is perceptible. In

the case of data and fax connections, which involve a complicated handshaking procedure, cable offers clear advantages in terms of connection security. At the same time, however, only 15% of the world's population are connected to the global cable network.²¹

For certain applications, therefore, satellite systems will continue to offer advantages over cable in the long term. Here are some examples from the civilian sphere:

- National, regional and international telephone and data traffic in areas with a low volume of communications, i.e. in those places where the low rate of use would make a cable connection unprofitable;
- Temporary communications systems used in the context of rescue operations following natural disasters, major events, large-scale building sites, etc.;
- UN missions in regions with an underdeveloped communications infrastructure.
- Flexible/mobile business communications using very small earth stations (VSATs, see below).

This wide range of uses to which satellites are put in the communications sphere can be explained by the following characteristics: the footprint of a single geostationary satellite can cover almost 50% of the earth's surface—impassable regions no longer pose a barrier to communication. In the area concerned, 100% of users are covered, whether on land, at sea or in the air. Satellites can be made operational within a few months, irrespective of the infrastructure available on the spot, they are more reliable than cable and can be replaced more easily.

The following characteristics of satellite communications must be regarded as drawbacks: the relatively long delay times, the path attenuation, the shorter useful life, by comparison with cable, of 12 to 15 years, the greater vulnerability to damage and the ease of interception.

By using appropriate antennae microwaves can be very effectively focused, allowing cables to be replaced by microwave radio links. If the transmitting and the receiving antenna are not in

line of sight, but rather, as they are on the earth, on the surface of a sphere, then from a given distance onwards the receiving antenna, disappears below the horizon owing to the curvature of the earth. The two antennae are thus no longer in line of sight. This would apply, for example, to an intercontinental microwave radio link between Europe and the USA.

The antennae would have to be fitted to masts 1.8 km high in order for a link to be established. For this reason, an intercontinental microwave radio link of this kind is simply not feasible, setting aside the issue of the attenuation of the signal by air and water vapor. However, if a kind of mirror for the microwave radio link can be set up in a fixed position high above the earth in space, large distances can be overcome, despite the curvature of the earth, just as a person can see round corners using a traffic mirror. The principle described above is made workable through the use of geostationary satellites.

If a satellite is placed into a circular orbit parallel to the equator in which it circles the earth once every 24 hours, it will follow the rotation of the earth exactly. Looking up from the earth's surface, it seems to stand still at a height of roughly 36 000 km—it has a geostationary position. Most communications and television satellites are satellites of this type.

The transmission of signals via satellite can be described as follows:

- The signal coming from a cable is transmitted by an earth station equipped with a parabolic antenna to the satellite via an upward microwave radio link, the **uplink**.
- The satellite receives the signal, regenerates it and transmits it back to another Earth station via a downward microwave radio link, the **downlink**.
- From there, the signal is transferred back to a cable network.

In the case of mobile communications satellite telephones the signal is transmitted directly from the mobile communications unit to the satellite, from where it can be fed into a cable link, via an Earth station, or directly transmitted to a different mobile unit.

The Most Important Satellite Communication Systems

If necessary, communications coming from public cable networks (not necessarily state networks) are transmitted between fixed earth stations, via satellite systems of differing scope, and then fed back into cable networks. A distinction is drawn between the following forms of satellite systems:

- Global systems (e.g. INTELSAT).
- Regional (continental) systems (e.g. EUTELSAT).
- National systems (e.g. ITALSAT).

Most of these satellites are in a geostationary orbit; 120 private companies throughout the world operate some 1,000 satellites.²²

In addition, the far northern areas of the earth are covered by satellites in a highly elliptical orbit (Russian molnyia orbits) in which the satellites are visible to users in the far north for half their orbit. In principle, two satellites can provide full regional coverage,²³ which is not feasible from a geostationary position above the equator. In the case of the Russian Molnyia satellites, which have been in service as communications satellites since 1974 (prototype launched in 1964), three equidistant satellites orbit the earth once every 12 hours and thus guarantee continuous transmission of communications.²⁴

Alongside this, the global INMARSAT system—originally established for use at sea—provides a mobile communications system by means of which satellite links can be established anywhere in the world. This system also uses geostationary satellites. The worldwide satellite-based mobile telephone system Iridium, which employed a number of satellites placed at time intervals in low orbits, recently ceased operating on economic grounds (over-capacity).

There is also a rapidly expanding market for so-called VSAT links (VSAT—very small aperture terminal). This involves the use of very small earth stations with antennae with a diameter of between 0.9 and 3.7 meters, which are operated either by firms to meet their own needs (e.g. videoconferences) or by mobile service providers to meet short-term communications requirements (e.g. in connection with meetings).

In 1996, 200,000 very small earth stations were in operation around the world. Volkswagen AG operates 3,000 VSAT units, Renault 4,000, General Motors 100,000 and the largest European oil company 12,000. If the client does not arrange for encryption, communication is entirely open.

Through the positioning of satellites above the Atlantic, Indian and Pacific regions, these satellite systems cover the entire globe.

INTELSAT

INTELSAT (International Telecommunications Satellite Organization) was founded as an authority in 1964 with an organizational structure similar to that of the UN and with the commercial purpose of providing international communications. The members of the organization were state-owned telecommunications companies. Today, 144 governments are INTELSAT members. In 2001, INTELSAT will be privatized.

INTELSAT now operates a fleet of 20 geostationary satellites, which provide links between more than 200 countries and whose services are rented out to the members of INTELSAT. The members operate their own ground stations. Following the establishment of INTELSAT Business Service (IBS) in 1984, non-members (e.g. telephone companies, large firms, and international concerns) can also use the satellites. INTELSAT offers global services such as communications, television, etc. Telecommunications are transmitted via the C-band and the Ku-band.

INTELSAT satellites are the most important international telecommunications satellites, accounting for a very large proportion of the world market in such communications. The satellites cover the Atlantic, Indian and Pacific regions. Ten satellites are positioned above the Atlantic between 304°E and 359°E. The Indian region is covered by six satellites situated between 62°E and 110m.5°E and the Pacific region by three satellites situated between 174°E and 180°E. The high volume of traffic in the Atlantic region is covered by a number of individual satellites positioned at the relevant longitudes.

INTERSPUTNIK

In 1971 the international communications organization INTERSPUTNIK was founded by nine countries as an agency of the former Soviet Union with a task similar to that of INTELSAT. Today, INTERSPUTNIK is an international organization, which the government of any country can join. It now has 24 member countries (including Germany) and some 40 users (including France and the UK), which are represented by their post offices or national telecommunications companies. Its headquarters are in Moscow.

Telecommunications are transmitted via the C-band and the Ku-band. Its satellites (Gorizont, Express and Express A, owned by the Russian Federation, and LMI-1, the product of the Lockheed-Martin joint venture) also cover the entire globe: one satellite is positioned above the Atlantic region, with a second planned, three are positioned above the Indian region and two are positioned above the Pacific region.

INMARSAT

Since 1979 INMARSAT (Interim International Maritime Satellite) has provided, by means of its satellite system, worldwide mobile communications at sea, in the air and on land and an emergency radio system. INMARSAT was set up as an international organization at the instigation of the International Maritime Organization. INMARSAT has since been privatized and has its headquarters in London.

The INMARSAT system consists of nine satellites in geostationary orbits. Four of these satellites—the INMARSAT-III generation—cover the entire globe with the exception of the high polar areas. Each individual satellite covers roughly one-third of the earth's surface. Through their positioning above the four ocean regions (West and East Atlantic, Pacific, Indian Ocean), global coverage is provided. At the same time, each INMARSAT has a number of spot beams, which make it possible to focus energy in areas with heavier communications traffic. Telecommunications are transmitted via the L-band and the Ku-band.

PANAMSAT

PanAmSat was founded in 1988 as a commercial provider of a global satellite system and has its headquarters in the USA. PanAmSat now has a fleet of 21 satellites, which provide services such as television, Internet and telecommunications on a worldwide basis, albeit chiefly in the USA. Telecommunications are transmitted via the C-band and the Ku-band. Of the 21 satellites, seven cover the Atlantic region, two the Pacific region and two the Indian Ocean region. The footprints of the remaining satellites cover North and South America. The PanAmSat satellites play only a secondary role in communications in Europe.

Regional Satellite Systems

The footprints of regional satellite systems cover individual regions/continents. As a result, the communications transmitted via them can be received only in those regions.

EUTELSAT

EUTELSAT was founded in 1977 by 17 European postal administrations with the aim of meeting Europe's specific satellite communication requirements and supporting the European space industry. It has its headquarters in Paris and some 40-member countries. EUTELSAT is to be privatized in 2001.

EUTELSAT operates 18 geostationary satellites, which cover Europe, Africa and large parts of Asia and establish a link with America. The satellites are positioned between 12.5°W and 48°E. EUTELSAT mainly offers television (850 digital and analog channels) and radio (520 channels) services, but also provides communication links—primarily within Europe, including Russia, e.g. for videoconferences—for the private networks run by large undertakings (including General Motors and Fiat), for press agencies (Reuters, AFP), for providers of financial information and for mobile data transmission services. Telecommunications are transmitted via the Ku-band.

ARABSAT

ARABSAT is the counterpart to EUTELSAT in the Arab region and was founded in 1976. Membership is made up of 21 Arab countries. ARABSAT satellites are used both for the transmission of television services and for communications. Telecommunications are transmitted mainly via the C-band.

PALAPA

The Indonesian PALAPA system has been in operation since 1995 and is the south-Asian counterpart to EUTELSAT. Its footprint covers Malaysia, China, Japan, India, Pakistan and other countries in the region. Telecommunications are transmitted via the C-band and the Ku-band.

National Satellite Systems

Many states meet their own requirements by operating satellite systems with restricted footprints.

One purpose of the French telecommunications satellite TELECOM is to link the French departments in Africa and South America with mainland France. Telecommunications are transmitted via the C-band and the Ku-band.

ITALSAT operates telecommunications satellites, which cover the whole of Italy by means of a series

of restricted footprints. Reception is therefore possible only in Italy. Telecommunications are transmitted via the Ku-band.

AMOS is an Israeli satellite whose footprint covers the Middle East. Telecommunications are transmitted via the Ku-band.

The Spanish HISPASAT satellites cover Spain and Portugal (KU-spots) and transmit Spanish television programs to North and South America.

The Allocation of Frequencies

The International Telecommunications Union (ITU) is responsible for the allocation of frequencies. For ease of organization, for radio communication purposes the world has been divided into three regions:

1. Europe, Africa, former Soviet Union, Mongolia;
2. North and South America and Greenland;
3. Asia, with the exception of countries in region 1, Australia and the South Pacific.

This division, which has become established over the years, was taken over for the purposes of satellite communications and has led to the positioning of large numbers of satellites in certain geostationary areas. The most important frequency bands for satellite communications are:

- The L-band (0.4 Æ 1.6 GHz) for mobile satellite communications, e.g. via IMMARSAT;
- The C-band (3.6 Æ 6.6 GHz) for earth stations, e.g. via INTELSAT;
- The Ku-band (10 Æ 20 GHz) for earth stations, e.g. INTELSAT Ku-spot and EUTELSAT;
- The Ka-band (20 Æ 46 GHz) for earth stations, e.g. military communications satellites;
- The V-band (46 Æ 56 GHz) for very small earth stations (VSATs).

The footprint is the area on the earth covered by a satellite antenna. It may embrace up to 50% of the earth's surface, or, by means of signal focusing, be restricted to small, regional spots. The higher the frequency of the signal emitted, the more it can be

focused and the smaller the footprint becomes. The focusing of the satellite signal on smaller footprints can increase the energy of the signal. The smaller the footprint, the stronger the signal, and thus the smaller the receiving antennae may be.

Parabolic antennae with a diameter of between 0.5 and 30m are used as receiving antennae on the earth. The parabolic mirror reflects all incoming waves and focuses them. The actual receiving system is situated in the focal point of the parabolic mirror. The greater the energy of the signal at the receiving point is, the smaller the diameter of the parabolic antenna need be.

The footprints of the INTELSAT satellites are divided into various beams. Each satellite's global beam (G) covers roughly one-third of the earth's surface; the hemispheric beams (H) each cover an area slightly smaller than half that covered by the global beams. Zone beams (Z) are spots in particular areas of the earth; they are smaller than the hemi-beams. In addition there are so-called spot beams; these are small, precise footprints.

The key factor in connection with the investigations conducted for this report is that a proportion of intercontinental communications are transmitted via the C-band in the global beams of the INTELSAT satellites and other satellites (e.g. INTERSPUTNIK) and those satellite antennae with a diameter of roughly 30-m are needed to receive some of these communications. Antennae of that size were also needed for the first stations set up to intercept satellite communications, since the first generation of INTELSAT satellites had only global beams and signal transmission technology was much less sophisticated than it is today. These antennae, some of which have a diameter of more than 30 m, are still used at the stations in question, even though they are no longer required on purely technical grounds. Today, the typical antennae required for INTELSAT communications in the C-band have a diameter of between 13 and 20 m.

Antennae with a diameter of between 2 and 5 m are required for the Ku-spots of the INTELSAT satellites and other satellites (EUTELSAT Ku-

band, AMOS Ku-band, etc.). In the case of very small earth stations, which operate in the V-band and whose signal, by virtue of the high frequency, can be focused even more strongly than those in the Ku-band, antennae with a diameter of between 0.5 and 3.7 m are adequate (e.g. VSATs from EUTELSAT or INMARSAT).

Satellite Communications for Military Purposes

Communications satellites play an important role in the military sphere as well. Many countries, including the USA, the United Kingdom, France and Russia, operate their own geostationary military communications satellites, with the aid of which independent global communication is possible. The USA has stationed one satellite roughly every 10° around the earth in some 32 orbital positions. However, some use is also made of commercial geostationary satellites for the purposes of providing military communications.

The frequency bands used for military communications lie in the range between 4 GHz and 81 GHz. The bands typically used by military communications satellites are X-band (SHF - 3-30 GHz) and the Ka-band (EHF - 20-46 GHz).

A distinction must be drawn between mobile stations, which may have a diameter of only a few decimeters, and fixed stations, which generally have a diameter not exceeding 11m. There are, however, two types of antenna (to receive signals from DSCS satellites) with a diameter of 18m.

The US MILSTAR program (Military Strategy, Tactical and Relay Satellite System), which operates six geostationary satellites worldwide, enables US armed forces to communicate with each other and with command centers using small earth stations, aircraft, ships and man-packs. Through the link among the satellites themselves worldwide communications availability is guaranteed even if all the US earth stations cease operating.

The DSCS (Defense Satellite Communications System) also provides global communications by means of five geostationary satellites. The US armed forces and some use the system government agencies.

The British military satellite system SKYNET also provides global communications. The French system SYRACUSE, the Italian system SICRAL and the Spanish system fly piggy-back on their respective national civilian communications satellites and provide military communications, albeit only on a regional basis, in the S-band. The Russians guarantee their armed forces' communications by means of transponders in the X-band used by the Molnya satellites.

NATO operates its own communications satellites (NATO IIID, IVA and IVB). The satellites provide voice, telex and data links between military units.

Clues to the Existence of at Least One Global Interception System

It is only natural that secret services do not disclose details of their work. Consequently there is, at least officially, no statement by the foreign intelligence services of the UKUSA states that they work together to operate a global interception system. The existence of such a system thus needs to be proved by gathering as many clues as possible, thereby building up a convincing body of evidence.

The trail of clues which constitutes evidence of this kind is made up of three elements:

- Evidence that the foreign intelligence services in the UKUSA states intercept private and business communications;
- Evidence that interception stations operated by the UKUSA states are to be found in the parts of the world where they would be needed in the light of the technical requirements of the civilian satellite communication system;
- Evidence that there is a closer than usual association between the intelligence services of these states.

For the purposes of proving the existence of such an association, it is irrelevant whether this extends to the acceptance from partners of applications for the interception of messages, which are then forwarded to them in the form of unevaluated raw material. This question is only relevant when investigating the hierarchies within such an interception association.

At least in democracies, intelligence services work on the basis of laws, which define their purpose and/or powers. It is thus easy to prove that in many of these countries foreign intelligence services exist which intercept civilian communications. This is true of the five UKUSA states, which all operate such services. There is no need for specific additional proof that any of these states intercept communications entering and leaving their territory.

Satellite communications also permit some intelligence communications intended for recipients abroad to be intercepted from the country's own territory. In none of the five UKUSA states is there any legal impediment to intelligence services doing this. The logic underlying the method for the strategic monitoring of foreign communications, and its at least partly overtly acknowledged purpose, make it practically certain that the intelligence services do in fact use it to that end.

The only restriction on the attempt to build up worldwide monitoring of satellite communications arises from the technical constraints imposed by these communications themselves. There is no place from which all satellite communications can be intercepted. It would be possible for a worldwide interception system to be constructed, subject to three conditions:

- The operator has national territory of its own in all the necessary parts of the world;
- The operator has, in all the necessary parts of the world, either national territory of its own or a right of access entitling it to operate or share the use of stations;
- The operator is a group of states, which has formed an intelligence association and operates the system in the necessary parts of the world.

None of the UKUSA states would be able to operate a global system on its own. The USA has, at least formally, no colonies. Canada, Australia and New Zealand also have no territory outside the narrower confines of their countries, and the UK would also not be able to operate a global interception system on its own.

On the other hand it has not been disclosed whether and to what extent the UKUSA states cooperate with one another in the intelligence field. Normally cooperation between intelligence services takes place bilaterally and on the basis of an exchange of evaluated material. A multilateral alliance is in itself something very unusual; if one adds to this the regular exchange of raw material, this would be a qualitatively new form of cooperation. The existence of such an association can only be proved on the basis of clues.

How Can a Satellite Communications Interception Station be Recognized?

Installations with large antennae belonging to the post office, broadcasting organizations or research institutions are accessible to visitors, at least by appointment; interception stations are not. They are generally operated, at least in name, by the military, which also carries out at least part of the technical work of interception. In the case of the stations run by the USA, for example, operations are carried out jointly with NSA by the Naval Security Group (NAVSECGRU), the United States Army Intelligence and Security Command (INSCOM) or the Air Intelligence Agency (AIA). In the British stations, the British intelligence service GCHQ operates the installations jointly with the Royal Air Force (RAF). This arrangement enables the installations to be guarded with military efficiency and at the same time serves as cover.

Various types of antennae are used in the installations, which fulfil criterion 1, each with a different characteristic shape, which provides evidence as to the purpose of the interception station. Arrangements of tall rod antennae in a large-diameter circle (Wullenweber antennae), for example, are used for locating the direction of

radio signals. Similarly, circular arrangements of rhombic-shaped antennae (Pusher antennae) serve the same purpose. Omnidirectional antennae, which look like giant conventional TV antennae, are used to intercept non-directional radio signals. To receive satellite signals, however, only parabolic antennae are used. If the parabolic antennae are standing on an open site, it is possible to calculate on the basis of their position, their elevation and their compass (azimuth) angle which satellite is being received. This is possible, for example, in Morwenstow (UK), Yakima (USA) or Sugar Grove (USA).

However, most often parabolic antennae are concealed under spherical white covers known as radomes: these protect the antennae, but also conceal which direction they are pointing in. If parabolic antennae or radomes are positioned on an interception station site, one may be certain that they are receiving signals from satellites, though this does not prove what type of signals these are.

Satellite receiving antennae on a site, which meets criterion 1, may be intended for various purposes:

- Receiving station for military communications satellites;
- Receiving station for spy satellites (pictures, radar);
- Receiving station for SIGINT satellites;
- Receiving station for interception of civilian communications satellites.

It is not possible to tell from outside what function these antennae or radomes serve. However, the diameter of the antennae gives some clues as to their purpose. There are minimum sizes, dictated by technical requirements, for antennae intended to receive the global beam in the C-band of satellite-based civilian international communications. The first generation of these satellites needed antennae with a diameter of 25-30 m; nowadays 15-20 m is enough. The automatic computer filtering of signals received calls for the highest possible signal quality, so for intelligence purposes an antenna at the upper end of the scale is chosen.

In the sphere of military communications as well, command centers have two types of antenna with a diameter of roughly 18 m (AN/FSC-78 and AN/FSC-79). However, most antennae for military communications have a much smaller diameter, since they must be transportable (tactical stations).

In view of the nature of the signals transmitted back to the station (high degree of focusing and high frequency), earth stations for SIGINT satellites need only small antennae. This also applies to antennae, which receive signals from spy satellites. If a site houses two or more satellite antennae with a diameter of at least 18-m, one of its tasks is certainly that of intercepting civilian communications. In the case of a station housing US forces, one of the antennae may also be used to receive military communications.

Official descriptions of the tasks of some stations have been published. In that connection governments and military units are regarded as official sources. If this criterion has been met, the others become superfluous.

Publicly Accessible Data About Known Interception Stations

With a view to determining which stations meet the criteria and thus form part of the global interception system and establishing what tasks they have, the relevant, somewhat contradictory, literature (Hager,²⁵ Richelson,²⁶ Campbell²⁷) declassified documents,²⁸ the homepage of the Federation of American Scientists and operators' homepages²⁹ (NSA, AIA, etc.) and other Internet publications were analyzed. In the case of the New Zealand station in Waihopai, the New Zealand Government has drawn up an official description of its tasks.³⁰ In addition, the footprints of telecommunications satellites were collated, the requisite antenna sizes were calculated and these footprints and antenna locations were entered, along with the locations of possible stations, on world maps.

The following principles relating to the physics of satellite communications apply in connection with the analysis:

- A satellite antenna can only record communications transmitted within the footprint in which it is located. In order to receive communications, which are mainly transmitted in the C-band and Ku-band, an antenna must lie within the footprints containing those bands.
- A satellite antenna is required for each separate global beam, even if beams from two satellites overlap.
- If a satellite has other footprints in addition to the global beam, which is typical of today's generations of satellites, a single satellite antenna can no longer record all the communications transmitted via that satellite, since a single satellite antenna cannot be located in every one of the satellite's footprints. In order to capture a satellite's hemispheric beam and its global beam, therefore, two satellite antennae are required in different areas.

If further beams (zone and spot beams) are involved, further satellite antennae are required. In principle, different, overlapping from a single satellite can be captured by one satellite antenna, since it is technically feasible to separate different frequency bands when reception takes place, although this leads to deterioration in the signal-noise ratio.

In addition, the non-accessibility of the installations, on the grounds that they are operated by the military,³¹ the fact that parabolic antennae are required to receive satellite signals and the fact that the size of the satellite antennae needed to capture the C-band in the global beam at least 30 m for the first INTELSAT generation and more than 15 to 18 m for later generations and the official descriptions of the tasks of some of the stations have been cited as evidence of their role in interception operations.

A global interception system must grow as communications develop. Accordingly, the start of the satellite communications era must lead to the establishment of stations and the introduction of new generations of satellites must lead to the establishment of new stations and the building of new satellite antennae which can cope with the new

technical requirements. The number of stations and the number of satellite antennae must increase whenever this is necessary in order to cover the full volume of communications traffic.

If we turn this equation round, it is no coincidence that, when new footprints come into being, new stations are established and new satellite antennae is built. Instead, this can be seen as a clue to the existence of a communications interception station.

Since the INTELSAT satellites were the first telecommunications satellites, and, moreover, the first to cover the entire globe, it is only logical that the introduction of the new generations of INTELSAT satellites should go hand-in-hand with the establishment of new and bigger stations. As long ago as 1965 the first INTELSAT satellite (Early Bird) was placed in a geostationary orbit. Its transmission capacity was still low and its footprint covered only the Northern Hemisphere.

When the second and third INTELSAT generations came into operation, in 1967 and 1968 respectively, global coverage was achieved for the first time. The satellites' global beams covered the Atlantic, Pacific and Indian Ocean areas. Satellite systems with smaller footprints had not yet been introduced. Three satellite antennae were thus needed in order to record all communications. Since two of the global beams overlapped over the European continent, in that area the global footprints of two satellites could be covered by two satellite antennae trained in different directions.

In addition, there are further stations which, although they do not meet the criterion of antenna size, and although there is no other clear evidence underpinning the assumption, may still form part of the global interception system. These stations could be used to cover the zone or spot beams of satellites whose global beams are intercepted by other stations or for whose global beam no large satellite antennae are required.

The Stations in Detail

In the detailed descriptions of the stations a distinction is drawn between stations, which are clearly used to intercept transmissions from telecommunications satellites and stations whose role cannot definitely be proven with the aid of those criteria.

The following stations meet the criteria, which point to a role in intercepting transmissions from telecommunications satellites.

Yakima, USA (120°W, 46°N)

The station was established in the 1970s, at the same time as the first generation of satellites were put into orbit. Since 1995, the Air Intelligence Agency (AIA), 544th Intelligence Group (Detachment 4), has been stationed in Yakima, along with the Naval Security Group (NAVSECGRU). Six satellite antennae have been installed on the site; the sources give no clue as to the size of the antennae. Hager describes the antennae as large and claims that they are trained on INTELSAT satellites over the Pacific (two satellite antennae) and INTELSAT satellites over the Atlantic, and on INMARSAT Satellite 2.

The fact that Yakima was established at the same time as the first generation of INTELSAT satellites went into orbit, and the general description of the tasks of the 544th Intelligence Group, suggest that the station has a role in global communications surveillance. A further clue is provided by Yakima's proximity to a normal satellite receiving station, which lies 100 miles to the north.

Sugar Grove, USA (80°W, 39°N)

Sugar Grove was established at the same time as the second generation of INTELSAT satellites came into operation, in the late 1970s. The NAVSECGRU and the AIA, 544th Intelligence

Group (Detachment 3) are stationed at Sugar Grove. According to information provided by a variety of authors, the station has 10 satellite antennae, three of which have a diameter greater than 18 m (18.2 m, 32.3 m and 46 m) and which are thus clearly used to intercept transmissions from telecommunications satellites. One of the tasks performed at the station by Detachment 3 of the 544th IG is to provide intelligence support for the collection by Navy field stations of information transmitted by telecommunications satellites.³² In addition, Sugar Grove is situated close (60 miles) to the normal satellite receiving station in Etam.

Sabana Seca, Puerto Rico (66°W, 18°N)

NAVSECGRU was first stationed in Sabana Seca in 1952. In 1995, it was joined by the AIA, 544th IG (Detachment 2). The station has at least one satellite antenna with a diameter of 32 m and four further small satellite antennae. According to official information, the station's tasks are to perform 'satellite communication processing', to provide 'cryptologic and communications service' and to support Navy and DoD operations, including the collection of COMSAT information (from a description of the 544th IG). In the future, Sabana Seca is set to become the first field station for the analysis and processing of satellite communications.

Morwenstow, England (4°W, 51°N)

Like Yakima, Morwenstow was established in the early 1970s, at the same time as the first generation of INTELSAT satellites went into space. The British Intelligence Service (GCHQ) operates Morwenstow. The Morwenstow site houses some 21-satellite antennae, three of which have a diameter of 30 m; no details are available of the size of the other antennae. No official information has been issued regarding the station's role; however, the size and number of the satellite antennae and the location of the station, only 110 km from the telecommunications station in Goonhilly, leave no doubt as to its task of intercepting transmissions from telecommunications satellites.

Menwith Hill, England (2°W, 53°N)

Menwith Hill was established in 1956 and by 1974 already housed eight satellite antennae. Today, the figure is roughly 30, some 12 of which have a diameter of more than 20 m. At least one of the large antennae, although certainly not all, is a receiving antenna for military communications (AN/FSC-78). The British and Americans work together at Menwith Hill. The US services stationed there are NAVSECGRU, the AIA (451st IOS) and INSCOM, which has command of the station. The land on which Menwith Hill stands belongs to the UK Defense Ministry and is rented to the US Administration. According to official information, Menwith Hill's role is "to provide rapid radio relay and to conduct communications research." According to statements by Richelson and the Federation of American Scientists, Menwith Hill is both an earth station for spy satellites and an interception station for transmissions from Russian telecommunications satellites.

Geraldton, Australia (114°O, 28°S)

The station was established in the early 1990s. It is run by the Australian Secret Service (DSD), and it is partly manned by British servicemen previously stationed in Hong Kong. According to Hager, four satellite antennae, of the same size (diameter of roughly 20 m) are trained on satellites above the Indian Ocean and the Pacific. According to statements made under oath in the Australian Parliament by an expert, transmissions from civilian telecommunications satellites are intercepted at Geraldton.³³

Pine Gap, Australia (133°O, 23°S)

The station in Pine Gap was established in 1966. It is run by the Australian Secret Service (DSD), and roughly half of the 900 station personnel are Americans from the CIA and NAVSECGRU. Pine Gap has 18 satellite antennae, one with a diameter of roughly 30 m and another with a diameter of roughly 20 m. According to official sources, and information provided by various authors, since its

inception Pine Gap has been an earth station for SIGINT satellites. Station personnel control and guide various spy satellites and receive, process and analyze their signals. The large satellite antennae also suggest that transmissions from telecommunications satellites are intercepted, since no such antennae are required for work with SIGINT satellites. Until 1980 no Australians were allowed to work in the signals analysis department; since then, they have been granted free access to all parts of the station, with the exception of the Americans own cryptography room.

Misawa, Japan (141°O, 40°N)

The station in Misawa was established in 1948 as the site for an HFDF antenna. Japanese and Americans man it. The US services represented are NAVSECGRU, INSCOM and some AIA groups (544th IG, 301st IS). The site houses around 14 satellite antennae, some of which have a diameter of roughly 20-m (estimate). Officially, Misawa acts as a “cryptology operations Center.” According to information supplied by Richelson, the station is used to intercept transmissions from the Russian Molnya satellites and other Russian telecommunications satellites.

Waihopai, New Zealand (173°O, 41°S)³⁴

Waihopai was established in 1989. It started with one large antenna, with a diameter of 18 m, and two smaller antennae were added later. According to Hager, the antennae are trained on INTELSAT 701 in orbit above the Pacific. Official information released by the GCSB (General Communications Security Bureau) Waihopai’s task is to intercept transmissions from communications satellites and to decrypt and process the signals.³⁵ Since the station has only two satellite antennae, the New Zealand secret service can intercept only a small proportion of communications in the pacific region. To serve any purpose, therefore, the station must work jointly with other stations in the region. Hager often names Geraldton in Australia as Waihopai’s “sister station.”³⁶

Hong Kong (22°N, 114°O)

The station was established in the late 1970s, at the same time as the second generation of INTELSAT satellites was put in space, and was equipped with large satellite antennae. No details are available of the exact sizes. In 1994, a start was made on the decommissioning of the station; the antennae were taken to Australia. It is not clear which station (Geraldton, Pine Gap or Misawa, Japan) has taken over the Hong Kong station’s tasks, which may have been divided among several stations.

Further Stations

The roles of the following stations cannot be clearly established on the basis of the criteria referred to above:

Leitrim, Canada (75°W, 45°N)

Leitrim is part of an exchange program between Canadian and US military units. According to the Navy, therefore, some 30 persons are stationed in Leitrim. In 1985 the first of four satellite antennae was installed, of which the two larger have a diameter of no more than roughly 12 m (estimate). According to official information, the station’s task is to provide “cryptologic rating” and to intercept diplomatic communications.

Bad Aibling, Germany (12°O, 47°N)

At present roughly 750 Americans work at the station near Bad Aibling. INSCOM (66th IG, 718th IG) which has the command, NAVSECGRU, and various AIA groups (402ndIG, 26th IOG) are stationed in Bad Aibling. The station has 14 satellite antennae, none of which has a diameter of more than 18 m. According to official information, Bad Aibling has the following tasks: “Rapid Radio Relay and Secure Common, Support to DoD and Unified Commands, Medium and Longhand Common HF & Satellite, Communication Physics Research, Test and Evaluate Common Equipment.” According to Richelson, Bad Aibling

is an earth station for SIGINT satellites and a listening station for transmissions from Russian telecommunications satellites. In accordance with a Department of Defense decision, the station is to be closed on 30 September 2002. Personnel will be transferred to other units.³⁷

Ayios Nikolaos, Cyprus (32°O, 35°N)

Ayios Nikolaos on Cyprus is a British station. The station, which has 14 satellite antennae whose size is unknown, is manned by two units, the 'Signals Regiment Radio and the Signals Unit (RAF)'. The station's location, close to the Arab states, and the fact that Ayios Nikolaos is the only station sited within certain footprints (above all spot beams) in this area, point to its having an important role in intelligence gathering.

Shoal Bay, Australia (134°O, 13°S)

Shoal Bay is a station run solely by the Australian Intelligence Service. The station reportedly has 10 satellite antennae; no official information is available regarding their size. Of the satellite antennae visible on photographs, the five larger ones have a maximum diameter of 8 m, and the sixth antenna visible is smaller still. According to information provided by Richelson, the antennae are trained on the Indonesian PALAPA satellites. It is not clear whether the station is part of the global system for the interception of civilian communications.

Guam, Pacific (144°O, 13°S)

Guam was established in 1898. It now houses a Naval Computer and Telecommunications Station manned by the 544th IG of the AIA and Navy soldiers. The station has at least four satellite antennae, two of which have a diameter of roughly 15-m.

Kunia, Hawaii (158°W, 21°N)

NAVSECGRU and the AIA have operated this station since 1993 as a Regional Security Operations Center (RSOC). Its tasks include the

provision of information and communications and cryptological support. Its broader role is not clear.

Buckley Field, Denver, Colorado, USA (104°W, 40°N)

The station was established in 1972 and is home to the 544th IG (Detachment 45). The site houses at least six satellite antennae, four of which have a diameter of roughly 20-m. The station's official task is to collect, process and analyze data about nuclear events obtained by SIGINT satellites.

Medina Annex, Texas, USA (98°W, 29°N)

Like Kunia, Medina, which was established in 1993, is an RSOC operated by NAVSECGRU and AIA units with tasks in the Caribbean.

Fort Gordon (81°W, 31°N)

Fort Gordon is also an RSOC, operated by INSCOM and the AIA (702nd IG, 721st IB, 202nd IB, 31st IS), whose tasks are unclear.

Fort Meade, USA (76°W, 39°N)

Ford Meade is the headquarters of the NSA.

The following conclusions can be drawn from the information collected concerning the stations and satellites and from the requirements outlined above:

1. In each footprint there are interception stations which cover at least some of the global beams and are equipped with at least one antenna with a diameter greater than 20 m. They are stations which are operated by the Americans or British or where American or British servicemen carry out intelligence activities.
2. The expansion of INTELSTAT communications and the establishment, at the same time, of the corresponding interception stations show that the system is intended to provide global coverage.
3. According to official information, some of these stations have the task of intercepting transmissions from communications satellites.

-
4. The information regarding stations contained in the declassified documents can be regarded as proof of the existence and activities of the stations concerned.
 5. Some stations are located in the areas covered by the beams or spots of several satellites, so that a large proportion of the relevant communications can be intercepted.
 6. There are some other stations, which, although they have no large antennae, may also be part of the system, since they can receive communications from the beams and spots. In this case, evidence other than the size of the antennae must be adduced.
 7. Some of the stations are situated in immediate proximity to normal earth stations for telecommunications satellites.

The UKUSA Agreement

A SIGINT agreement signed in 1948 between the United Kingdom, the United States and Australia, Canada and New Zealand is referred to as the UKUSA Agreement.³⁸ The UKUSA Agreement represents a continuation of the cooperation between the USA and the UK, which dates back to the First World War and which became very close during the Second World War.

It was the Americans who instigated the establishment of a SIGINT alliance at a meeting with the British in London in August 1940.³⁹ In February 1941, US code breakers delivered a cipher machine (PURPLE) to the United Kingdom. Cooperation in the sphere of code breaking began in spring 1941.⁴⁰ Intelligence cooperation was stepped up in response to the joint fleet operations in the North Atlantic in summer 1941. In June 1941 the British broke the German fleet code, ENIGMA.

America's entry into the war led to SIGINT cooperation being stepped up. In 1942, US code breakers from the Naval SIGINT Agency began work in the United Kingdom.⁴¹ Liaison between the submarine tracking rooms in London, Washington and, from May 1943 onwards, Ottawa in Canada was so close that, according to a

statement by one individual involved at the time, they worked like a single organization.⁴²

In spring 1943 the BRUSA-SIGINT Agreement was signed, and personnel were exchanged. The agreement primarily concerns the division of work and its main substance is summarized in the first three paragraphs: they cover the exchange of all information obtained by means of the discovery, identification and interception of signals and the cracking of codes and encryption processes. The Americans were primarily responsible for Japan, the British for Germany and Italy.⁴³

Following the war, the UK was the prime mover behind the continuation of a SIGINT alliance. The foundations were laid in the course of a world tour undertaken in spring 1945 by British intelligence agents, including Sir Harry Hinsley. One aim was to transfer SIGINT personnel from Europe to the Pacific to take part in the war against Japan. In that connection, an agreement was reached to provide the Australian intelligence services with resources and personnel (British). The intelligence agents returned to the USA via New Zealand and Canada.

In September 1945 Truman signed a top-secret memorandum whose provisions formed the cornerstone of a peacetime SIGINT alliance.⁴⁴ Immediately thereafter, negotiations on an agreement opened between the British and Americans. In addition, a British delegation made contact with the Canadian and Australians with a view to discussing their involvement.

In February and March 1946 a top-secret Anglo-American SIGINT conference took place at which the details of an alliance were discussed. The British were authorized by the Canadians and Australians to act on their behalf. The conference produced what was still a classified agreement, running to some 25 pages, which laid down the detailed arrangements for a SIGINT agreement between the United States and the British Commonwealth. Further discussions took place during the two following years, culminating in the signing of the definitive text of the UKUSA Agreement in June 1948.⁴⁵

For a long time, the signatory states refused officially to acknowledge the existence of the UKUSA Agreement. However, the annual report of the Intelligence and Security Committee, the UK's parliamentary monitoring body refers explicitly to the agreement: "The quality of intelligence gathered clearly reflects the value of the close co-operation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as well as GCHQ's normal UK customers, were served directly from GCHQ."⁴⁶

A publication of the New Zealand Department of the Prime Minister from the year 2000, dealing with the management of the New Zealand's security and intelligence services, also refers clearly to the agreement: "The operation of the GCSB is directed solely by the New Zealand Government. It is, however, a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology. The other members of the partnership are the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ) Australia's Defense Signals Directorate (DSD) and Canada's Communications Security Establishment (CSE). New Zealand gains considerable benefit from this arrangement, as it would be impossible for New Zealand to generate the effectiveness of the five nation partnership on its own."⁴⁷ Moreover, there is further evidence of the agreement's existence.

According to the US Navy,⁴⁸ UKUSA stands for "United Kingdom-USA" and refers to a "5-nation SIGINT agreement."

The Head of the Australian Intelligence Service (DSD) confirmed the existence of the agreement in an interview: according to the information he gave, the Australian Secret Service cooperates with other overseas intelligence agencies under the UKUSA Agreement.⁴⁹

A Canadian Security and Intelligence Committee report describes how Canada cooperates with some

of its closest and longest-standing allies in the intelligence sphere. The report names the allies concerned: the United States (NSA), the United Kingdom (GCHQ), Australia (DSD) and New Zealand (GCSB). The report does not name the agreement.

In an interview with Christopher Andrew, a professor at Cambridge University, conducted in November 1987 and April 1992, the former Deputy Director of the NSA, Dr Louis Torella, who was present when the agreement was signed, confirmed that it does exist.⁵⁰

The former Head of GCHQ, Joe Hooper, refers to the UKUSA Agreement in a letter of 22 July 1969 to the former Director of the NSA, Marshall S. Carter.

Under the 1966 Freedom of Information Acts (5 USC § 552) and the Department of Defense's 1997 FOIA Regulation 5400.7-R, formerly classified documents were declassified and thus made available to the public.

The documents concerning the National Security Archive, founded in 1985 at George Washington University in Washington DC, are accessible to the public. The author Jeffrey Richelson, a former member of the National Security Archive, has published 16 documents on the Internet which give an insight into the emergence, development, management and mandate of the National Security Agency (NSA).⁵¹

In two of these documents, ECHELON is named. These documents have repeatedly been cited by various authors writing about ECHELON as evidence for the existence of the ECHELON global espionage system. The documents made available by Richelson also include some which confirm the existence of the National Reconnaissance Office and its function as a manager and operator of intelligence satellites.⁵² Following our conversation with Jeffrey Richelson in Washington he forwarded further declassified documents to the Temporary Committee. Those relevant to our investigations have been taken into account here.

The documents contain fragmentary descriptions of or references to the following topics:

- In National Security Council Intelligence Directive 9 (NSCID 9) of 10 March 1950 the term foreign communications is defined for COMINT purposes: it comprises any government communications in the widest sense (not only military) and all other communications, which might contain information of military, political, scientific or economic value.
- The Directive (NSCID 9 rev, 29.12.1952) expressly states that the FBI alone is responsible for internal security.
- The Department of Defense (DoD) Directive of 23 December 1971 on the NSA and the Central Security Service (CSS) outlines the concept for the NSA as follows:
 - The NSA is a separately organized office within the DoD headed by the Secretary of Defense;
 - The NSA's task is firstly to fulfil the USA's SIGINT mission, and secondly to provide secure communications systems for all departments and offices;
 - The NSA's SIGINT activities do not cover the production and distribution of processed intelligence: this is the sphere of other departments and offices.

The 1971 DoD Directive also sketches out the structure of the NSA and CSS. In its statement to the House Permanent Select Committee on Intelligence on 12 April 2000,⁵³ Gen. Michael Hayden, the NSA Director, defined the NSA's tasks as follows:

- Collecting foreign communications for the military and for policymakers by means of electronic surveillance;
- Supplying intelligence for US Government consumers about international terrorism, drugs and arms proliferation;
- The NSA does not have the task of collecting all electronic communications.

- The NSA may only pass on information to recipients authorized by government, not direct to US firms.

In a memorandum by Vice-Admiral W.O. Studeman of the US Navy on behalf of the Government on 8 April 1992,⁵⁴ reference was made to the increasingly global access of the NSA in addition to ,support of military operations.

Powers of the Intelligence Agencies⁵⁵

It is clear from US Signals Intelligence Directive 18 (USSID 18) that both cable and radio signals are intercepted. The duties of the US Communications Intelligence Board include monitoring all arrangements with foreign governments in the COMINT field. One of the tasks of the NSA Director is to arrange all contacts with foreign COMINT services.⁵⁶

The NAVSECGRU Instructions C5450.48A⁵⁷ describe the duties, function and purpose of the Naval Security Group Activity (NAVSECGRUACT), 544th Intelligence Group, in Sugar Grove, West Virginia. They state that one particular task is to maintain and operate an ECHELON site; they also mention that one task is the processing of intelligence information.

In the document "History of the Air Intelligence Agency" (1 January to 31 December 1994)⁵⁸ the Air Intelligence Agency (AIA), Detachment 2 and 3, is mentioned under the heading, Activation of ECHELON Units.

These documents do not give any information on what an 'ECHELON site' is, what is done at an 'ECHELON site', or what the codename ECHELON stands for. These documents do not reveal anything about the UKUSA Agreement.

Information From Authors and Journalists

The ECHELON system was first described in detail in the book, *Secret Powers: New Zealand's role in the international spy network*, published in 1996 by the New Zealand author Nicky Hager. He draws

on interviews with more than 50 persons who were employed by the New Zealand intelligence service, GCSB, or otherwise involved in intelligence activities. He also analyzed a wide range of documents from national archives, newspapers and other published sources. According to Hager, the global interception system is referred to as ECHELON, and the network computers as ECHELON Dictionaries.

According to Hager, the origins of cooperation between intelligence services under the UKUSA Agreement can be traced back to 1947, when, following their cooperation in the war, the UK and USA concluded an agreement on continuing COMINT activities on a joint basis around the globe, under which the two countries were to cooperate on the creation of an interception system providing the maximum possible global coverage, share the special installations required and the associated costs and pool the fruits of their labors. Canada, Australia and New Zealand subsequently signed up to the UKUSA agreement.

Hager says that interception of satellite communications is the core activity of the current system. The interception by ground stations of messages sent via Intel satellites began in the 1970s. The computer searches such messages for specific keywords and/or addresses in order to filter out the relevant communications. Surveillance activity was later extended to other satellites, such as those of Inmarsat,⁵⁹ which concentrated on maritime communications.

In his book, Hager points out that the interception of satellite communications represents only a small, albeit important, part of the eavesdropping system, for there are also numerous facilities for monitoring microwave and cable links, although these are less well documented and their existence is more difficult to prove, since, unlike ground stations, they are rather inconspicuous. ECHELON is thus synonymous with a global eavesdropping system.

In his statement to the Temporary Committee, made on 24 April 2001, Hager emphasized that the interception system was not all-powerful. Since

the limited resources had to be used as effectively as possible, not all communications could be intercepted, but rather only those likely to offer up important information. For that reason, the communications targeted were those of political and diplomatic interest. If communications were intercepted with a view to obtaining economic intelligence, the information concerned the macro—rather than the microeconomic sphere.

As far as the interception system's operating methods were concerned, each partner state had its own list of search words on the basis of which communications were intercepted. In addition, however, the USA using "dictionary managers" screened communications for keywords entered into the system. The British therefore had no control over the screening process and had no idea what information was collected in Morwenstow, since it was forwarded directly to the USA. In that connection, Hager emphasized the risk posed to continental Europe by the British interception stations.

Citing several examples, he pointed out that the UKUSA partner states were spying on allies and trading partners in the Pacific. The only countries not being spied on were the UKUSA partner states themselves. In Hager's view, like their New Zealand counterparts the British secret services would probably be very loath to call the UKUSA partnership into question by refusing to cooperate and intercept communications originating from continental Europe. There would be no reason for the United Kingdom to forfeit information of interests to its intelligence services, and, since that information would always remain secret, espionage under the UKUSA Agreement would not rule out an official policy of loyalty vis-à-vis Europe.

In his many publications the British journalist Duncan Campbell draws on the work of Hager and Richelson, on conversations with former intelligence service staff and on other research. According to his statements, ECHELON is part of the global system, which intercepts and analyses international satellite communications. Each partner state uses 'dictionary' computers, which screen the intercepted messages for keywords.

In STOA Study 2/5 of 1999, which provides an in-depth analysis of the technical aspects, Campbell describes in detail how any medium used for transmitting information can be intercepted. In one of his latest writings, however, he makes it clear that even ECHELON has its limits and that the initial view that total monitoring of communications was possible has turned out to be erroneous. Neither ECHELON nor the signals intelligence system of which it is part can do this. Nor is equipment available with the capacity to process and recognize the content of every speech message or telephone call.

In his statement to the Temporary Committee, made on 22 January 2001, Campbell expressed the view that the USA used its intelligence services to help US firms win contracts. Relevant information was passed on to firms via the CIA with the assistance of the Advocacy Center and the Office of Executive Support in the Department of Commerce. In support of this argument he put forward documents providing evidence of intervention by the Advocacy Center to the benefit of US firms; moreover, much of the information concerned can be found on the homepage of the Advocacy Center. The claim that the success of the Advocacy Center is based on the interception of communications is speculation and is not supported by the documents.

Campbell emphasized that the interception capabilities of several European countries (e.g. Switzerland, Denmark, France) had increased substantially in recent years. The intelligence sector had also seen an expansion in bilateral and multilateral cooperation.

The US author, Jeffrey Richelson, a former member of the National Security Archives, has made available on the Internet 16 previously classified documents, which give an insight into the inception, development, management and remit of the National Security Agency. In addition, he is the author of various books and articles on the intelligence activities of the USA.

In his work he draws on many declassified documents, the research carried out by Hager and his own research. During his meeting with the delegation from the Temporary Committee, held in Washington DC on 11 May 2001, he stated that ECHELON referred to a computer network used to filter data which was then exchanged between intelligence services. In his 1985 book "The Ties That Bind" he describes in detail the negotiations which led up to the signing of the UKUSA Agreement and the activities under that agreement of the secret services of the USA, the United Kingdom, Canada, Australia and New Zealand.

In his very comprehensive 1999 book "The US Intelligence Community" he gives a survey of the USA's intelligence activities and describes the organizational structure of the intelligence services and their methods of collecting and analyzing information. In Chapter 8 of the book he examines in detail the SIGINT capabilities of the intelligence services and describes some earth stations. In Chapter 13 he outlines the USA's relations with other intelligence services, for example under the UKUSA Agreement.

In his article entitled "Desperately Seeking Signals," which appeared in 2000, he gives brief details of the substance of the UKUSA Agreement, names installations used to intercept transmissions from communications satellites and outlines the scope for and the limits on the interception of civilian communications.

US author James Bamford, whose work is based both on archive research and the questioning of intelligence service staff, was one of the first people to tackle the subject of the NSA's SIGINT activities. As long ago as 1982 he published the book "The Puzzle Palace," chapter 8 of which, entitled "Partners," describes the UKUSA Agreement in detail. According to his new book, "Body of Secrets," which builds on the findings outlined in "The Puzzle Palace," the computer network linking the intelligence services is known as "Platform." ECHELON is the name of the software used in all the relevant stations, providing for uniform processing of data and direct access to

the data held by other intelligence services. In the subsequent chapters, however, he also uses the term ECHELON to denote the interception system set up under the UKUSA Agreement.

In “Body of Secrets,” and in the chapter of most relevance to the work of the Temporary Committee, entitled “Muscle,” Bamford gives a historical survey of the development of communications surveillance by the NSA and describes the scope of the system, the way the UKUSA partnership operates and its objectives. He emphasizes that, according to interviews conducted with dozens of current and former NSA employees, the NSA is at present not involved in the work of gathering competitive intelligence.

He confirmed this statement when giving evidence to the Temporary Committee on 23 April 2001. The NSA could only be given the task of gathering competitive intelligence on the basis of a clear political decision taken at the very highest level, a decision, which has thus far not been taken. In the course of 20 years’ research, Bamford had never uncovered evidence of the NSA passing on intelligence to US firms, even though it intercepts communications from private firms, for example with a view to monitoring compliance with embargoes.

According to Bamford, the main problem for Europe is not the issue of whether the ECHELON system steals firms’ business secrets and passes them on to competitors, but rather that of the violation of the fundamental right to privacy. In “Body of Secrets” he describes in detail how the protection of ‘US persons’ (i.e. US citizens and persons legally resident in the USA) has developed and makes clear that at least internal restrictions have been laid down in respect of other UKUSA residents. At the same time, he points out that other persons enjoy no protection, that there is no requirement to destroy data concerning such persons, and that the NSA’s data storage capacities are unimaginably huge.

However, Bamford also emphasizes the limits of the system, which stem from the fact that, firstly, only

a small proportion of international communications are now transmitted via satellites—transmissions via fiber optic cable are much more difficult to intercept—and secondly, that the NSA has only limited capacities when it comes to the final analysis of intercepted communications. Moreover, those capacities must be set against an ever-increasing volume of communications, transmitted in particular via the Internet.

Bo Elkjaer and Kenan Seeburg, two Danish journalists told the Temporary Committee on 22 January 2001 that ECHELON was already very advanced in the 1980s. Denmark, which greatly expanded its interception capabilities in the 1990s, has been cooperating with the USA since 1984. Echoing their article in *Ekstra Bladet*,⁶⁰ in which they referred to an illustrated lecture (25 slides) given by an unnamed officer of the 544th Intelligence Group of the Air Intelligence Agency, they claimed that various NGOs (including the Red Cross) were also ECHELON targets.

Margaret Newsham⁶¹ was employed from 1974 to 1984 by Ford and Lockheed and says she worked for the NSA during that period. She had been trained for her work at NSA Headquarters at Fort George Meade in Maryland, USA, and had been deployed from 1977 to 1981 at Menwith Hill; the US ground station on UK territory. There she established that a conversation conducted by US Senator Strom Thurmond was being intercepted. As early as 1978, ECHELON was capable of intercepting telecommunications messages to and from a particular person via satellite.

As regards her role in the NSA, she was responsible for designing systems and programs, configuring them and preparing them for operation on powerful computers. The software programs were named SILKWORTH and SIRE, whilst ECHELON was the name of the network.

Wayne Madsen,⁶² former NSA employee, also confirms the existence of ECHELON. He is of the opinion that economic intelligence gathering has top priority and is used to the advantage of US companies. He fears in particular that

ECHELON could spy on NGOs such as Amnesty International or Greenpeace. He argues that the NSA had to concede that it held more than 1000 pages of information on Princess Diana, because her conduct ran counter to US policy, owing to her campaign against land mines. During his meeting with the committee delegation in Washington DC Madsen expressed particular concern at the risks to the privacy of European citizens posed by the global espionage system.

Mike Frost worked for more than 20 years for the CSE, the Canadian secret service.⁶³ The listening post in Ottawa was just one part of a worldwide network of spy stations.⁶⁴ In an interview with CBS, he said that all over the world, every day, telephone conversations, e-mails and faxes are monitored by ECHELON, a secret government surveillance network.⁶⁵ This also included civilian communications.

In an interview he gave for an Australian TV channel, he said by way of example that the CSE actually had entered the name and telephone number of a woman in a database of possible terrorists because she had used an ambiguous phrase in a harmless telephone conversation with a friend. When searching through intercepted communications, the computer had found the keyword and reproduced the conversation. The analyst was unsure and therefore recorded her personal details.⁶⁶

The intelligence services of the UKUSA states also helped each other by spying on each other's behalf so that at least local intelligence services could not be accused of anything. For instance, GCHQ asked the CSE to spy on two British government ministers when Prime Minister Thatcher wanted it to tell her if they were on her side.⁶⁷

Fred Stock says he was expelled from CSE, the Canadian secret service, in 1993 because he had criticized the new emphasis on economic intelligence and civil targets. The communications intercepted contained information on trade with other countries, including negotiations on NAFTA, Chinese purchases of cereals and

French arms sales. Stock says the service also routinely received communications concerning environmental protests by Greenpeace vessels on the high seas.⁶⁸

Information From Government Sources

James Woolsey, the former director of the CIA, said at a press conference⁶⁹ he gave at the request of US State Department, that the USA did conduct espionage operations in continental Europe. However, 95% of 'economic intelligence' was obtained by evaluating publicly accessible information sources, and only 5% came from stolen secrets. Espionage was used to secure economic intelligence from other countries where compliance with sanctions and dual-use goods were concerned, and in order to combat bribery in connection with the award of contracts. Such information is not, however, passed to US companies.

Woolsey stressed that, even if espionage yielded economically usable intelligence, it would take an analyst a very long time to analyze the large volume of available information, and that it would be wrong to use their time on spying on friendly trading partners. He also pointed out that, even if they did so, complex international interlinkages would make it difficult to decide which companies were US companies and thus should be allowed to have the information.

Answers to various questions in the House of Commons⁷⁰ reveal that the station at RAF Menwith Hill is owned by the UK Ministry of Defense, but is made available to the US Department of Defense, specifically the NSA,⁷¹ which provides the chief of station,⁷² as a communications facility.⁷³ In mid-2000, there were 415 US military, 5 UK military, 989 US civilian and 392 UK civilian personnel working at RAF Menwith Hill, excluding GCHQ staff present on the site.⁷⁴

The presence of US military personnel is governed by the North Atlantic Treaty and special confidential⁷⁵ administrative arrangements appropriate to the relationship, which exists between the governments of the UK and the USA for the purposes of common defense.⁷⁶ The

station is an integral part of the US Department of Defense's worldwide network, which supports the interests of the UK, the USA and NATO.⁷⁷

In the Intelligence and Security Committee's 1999/2000 annual report, emphasis is specifically placed on the value of the close cooperation under the UKUSA Agreement, as reflected in the quality of the intelligence gathered. It is pointed out in particular that when the NSA's equipment was out of action for some three days, US customers as well as UK customers were served direct from GCHQ.⁷⁸

Martin Brady, Director of the Australian intelligence service DSD,⁷⁹ confirmed in a letter to the "Sunday" program on Australia's Channel 9 that DSD cooperated with other intelligence services as part of the UKUSA Agreement. In the same letter, he stressed that all Australia's intelligence facilities were operated by Australian services alone or jointly with US services. Where use of such facilities is shared, the Australian Government has full knowledge of all activities and Australian personnel are involved at all levels.⁸⁰

A document published by the New Zealand Department of the Prime Minister in 2000, which deals with the role of the national security and intelligence services refers explicitly to the partnership between the intelligence services of the USA, the UK, Canada, Australia and New Zealand and emphasizes the benefits for New Zealand.⁸¹

On 19 January 2001, the Netherlands Minister for Defense presented a report to the Netherlands Parliament on technical and legal aspects of the global surveillance of modern telecommunications systems.⁸² In it, the Netherlands Government takes the view that, although it had no information of its own on this matter, it was highly likely, on the basis of available third-party information, that the ECHELON network did exist, but that there were also other systems with the same capabilities. The Netherlands Government came to the conclusion that global interception of communications systems was not confined to countries involved in the

ECHELON system, but was also carried on by government authorities of other countries.

Luigi Ramponi, former director of SISMI, the Italian intelligence service, leaves no room for doubt in the interview he gave for 'Il Mondo' that ECHELON does exist.⁸³ Ramponi says explicitly that, as Head of SISMI, he knew of Echelon's existence. Since 1992, he had been kept in the picture about intensive interception of low-, medium- and high frequencies. When he joined SISMI in 1991, most dealings were with the UK and the USA.

Parliamentary Reports

The Belgian monitoring committee, the Comité Permanent R, has already discussed ECHELON in two reports. The third chapter of its 1999 activity report was devoted to how the Belgian intelligence services are reacting to the possible existence of an ECHELON system of communications surveillance. The 15-page report concludes that both the Belgian intelligence services, the Sûreté de l'Etat and the Service General du Renseignement (SGR), only found out about ECHELON through documents in the public domain.

The second report deals with the ECHELON system in much greater detail. It gives a view on the STOA study and devotes one section to explaining the technical and legal background to telecommunications monitoring. It concludes that ECHELON does in fact exist and is also in a position to listen in to all information carried by satellite (approximately 1% of total international telephone communications), in that it searches for keywords, and that its decoding capacity is much greater than the Americans claim. Doubt remains about the accuracy of statements that no industrial espionage is carried out at Menwith Hill. The report makes it clear that it is impossible to ascertain with any certainty what ECHELON does or does not do.

The French National Assembly's Committee on National Defense has drawn up a report on surveillance systems. At the meeting held on 28

November 2000, Arthur Paecht, presented the report's findings to the Temporary Committee. Following a detailed discussion of a wide variety of aspects, Arthur Paecht came to the conclusion that ECHELON exists and is, in his view, the only known multinational surveillance system. The system's capacities are real but have reached their limits not only because the expenditure can no longer keep pace with the explosion in communications but also because certain targets now know how to protect themselves.

The ECHELON system has moved away from its original goals, which were linked to the Cold War, and this means that it is not impossible that the intelligence gathered may be used for political and industrial purposes against other NATO states. ECHELON might indeed present a danger to fundamental freedoms and in this context it raises numerous problems that demand appropriate answers. It would be wrong to imagine that the ECHELON member states will give up their activities. On the contrary, there are several indications of a new system being created with new partners as a way of acquiring additional resources to overcome Echelon's limits.

In Italy the parliamentary Committee on Intelligence and Security Services drew up a report entitled "The role of the intelligence and security services in the ECHELON case,"⁸⁴ which was forwarded to the President of the Italian Parliament on 19 December 2000. The conclusions concerning the existence of a system named ECHELON are vague.

According to the report, "during the hearings in committee the existence of an integrated interception system of that name, operated by the five signatory states to the UKUSA Agreement (USA, United Kingdom, Australia, New Zealand and Canada) and designed to intercept communications on a worldwide basis was largely ruled out." Although the existence of closer cooperation among the English-speaking countries was not in doubt, the committee had failed to find evidence that the cooperation was geared to the

establishment of an integrated interception system or even a worldwide interception network.

The committee felt it was likely that the name ECHELON denoted a stage reached in the development of technology for the interception of satellite communications. The report made explicitly clear that the Italian secret service SISMI had ruled out the existence of an automatic system for the recognition of words used in conversations, so that the targeted interception of conversations containing given keywords was not feasible.

Might There be Other Global Interception Systems?

Listening in to international communications transmitted by first-generation satellites requires receiving stations in the Atlantic, the Indian Ocean and the Pacific area. In the case of the newer generation of satellites, which can transmit to sub-regions, further requirements with regard to the geographical position of listening stations would have to be met if all communications via satellite were to be intercepted. Any other interception system operating on a global scale would be forced to establish its stations outside the territory of the UKUSA states.

The establishment of an interception system of this kind operating on a global scale would, however, also have to make economic and political sense for the operator or operators. The beneficiary or beneficiaries of such a system would have to have global economic, military or other security interests, or at least believe that they were among the world's superpowers. Consequently, we are essentially talking only about China and the G-8 States, excluding the United States and the United Kingdom.

France has its own territories, departments and regional authorities in all three areas listed above. In the Atlantic, there is St Pierre and Miquelon east of Canada (65° W/47° N), Guadeloupe, northeast of South America (61° W/16° N), and Martinique (60° W/14° N) and French Guyana on the northeast coast of South America (52° W/5° N).

In the Indian Ocean there is Mayotte to the east of southern Africa (45° E/12° S) and Réunion (55° E/20° S) and to the very south the French Southern and Antarctic Territories. In the Pacific there is New Caledonia (165° E/20° S), the Wallis and Futuna Islands (176° W/12° S) and French Polynesia (150° W/16° S).

Very little information is available about possible stations operated by the French intelligence service (DGSE) in these overseas areas. According to reports by French journalists,⁸⁵ there are stations in Kourou in French Guyana and in Mayotte. No details are available as to the size of the stations, the number of satellite antennae or their size. There are apparently other stations in France at Domme near Bordeaux and at Alluets-le-Roi near Paris. Vincent Jauvert estimates that there are a total of 30 satellite antennae. The author, Erich Schmidt-Eenboom⁸⁶ claims that a station is also operating in New Caledonia and is used by the German Federal Intelligence Service.

Theoretically, since it meets the geographical, technical and financial requirements, France could also operate a global interception system. However, there is insufficient information available in the public domain to seriously assume that this is the case.

The Russian intelligence service FAPSI (Federal Agency of Government Communications and Information, Federalnoye Agentstvo Pravitelstvennoy Svyazi), which is responsible for communications security and SIGINT, operates ground stations in Latvia, Vietnam and Cuba in cooperation with the Russian military intelligence service GRU. On the basis of the relevant legal provisions, FAPSI's role is to collect political, economic, military and scientific and technological information with a view to fostering economic, military and scientific and technological development.⁸⁷ In addition, in 1997 the Director of FAPSI described its primary tasks as the interception of encrypted foreign communications and global interception.

In the Atlantic area, the Federation of American Scientists claims that there is a facility at Lourdes in Cuba (82° W/23° N), which is operated jointly with the Cuban intelligence service. With the aid of this station, Russia both gathers strategic intelligence and intercepts military and commercial communications. In the Indian Ocean there are stations in Russia, about which no further information is available. A further station in Skudra in Latvia was closed in 1998.

In the Pacific there is apparently a station at Cam Rank Bay in North Vietnam. No detailed information is available about the stations as far as the number and size of the antennae are concerned. Together with the stations available in Russia itself, global coverage is theoretically possible. However, here too, the information available is insufficient to draw any firm conclusions.

Neither the other G-8 states nor China has territories or close allies in the parts of the world that would enable them to operate a global interception system.

Compatibility of an ECHELON Type Communications Interception System With Union Law

The committee's remit includes the specific task of examining the compatibility of an 'ECHELON' type communications interception system with Community law. In particular, it is to examine whether such a system complies with the two data protection Directives 95/46/EC and 97/66/EC, with Article 286 TEC, and Article 8(2) TEU. This matter has to be considered from two different angles.

The first arises from the circumstantial evidence, which indicates that the system known as "ECHELON" was designed as a communications interception system to provide the US, Canadian, Australian, New Zealand and British secret services with information about events abroad by collecting and evaluating communications data. As such, it

is a conventional espionage tool used by foreign intelligence services. Initially, therefore, we will examine the compatibility of such an intelligence system with Union law.

In addition, the STOA report by Duncan Campbell alleges that the system has been misused for purposes of obtaining competitive intelligence, causing serious losses to the industries of European countries. Furthermore, there are statements by the former CIA Director R. James Woolsey, that although the USA was spying on European firms, this was only to restore a level playing field since contracts had only been secured as a result of bribery. If it is true that the system is used to obtain competitive intelligence, the further issue arises of whether this is compatible with Community law.

In principle, activities and measures undertaken for the purposes of state security or law enforcement do not fall within the scope of the EC Treaty. On the basis of the principle of limited authority, the European Community can only take action where a corresponding competence has been conferred on it. The Community rightly excluded these areas from the scope of application of the data protection directives, which are based on the EC Treaty, and in particular Article 95 (ex-Article 100a) thereof.

Directive 59/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector do not apply to "the processing of data/activities concerning public security, defense, state security (including the economic well-being of the state when the activities relate to state security matters) and the activities of the state in areas of criminal law."⁸⁸

Exactly the same wording has been used in the proposal for a directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, which is currently before Parliament. The involvement of a Member State in an interception system for the

purposes of State security cannot therefore be in breach of the EC's data protection directives.

Similarly, there can be no breach of Article 286 TEC, which extends the scope of the data protection directives to data processing by Community institutions and bodies. The same applies to Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. This regulation is also applicable only in so far as the bodies are acting within the framework of the EC Treaty. To avoid misunderstandings, it should be clearly emphasized at this point that no sources whatsoever contend that there is any involvement of Community bodies and institutions in a surveillance system.

As far as the areas covered by Title V (common foreign and security policy) and Title VI (police and judicial cooperation in criminal matters) are concerned, there are no data protection provisions comparable to those of the EC directives. The European Parliament has already pointed out on numerous occasions that action is much needed in this area.⁸⁹

The protection of the fundamental rights and freedoms of the individual in these spheres is ensured only by Articles 6 and 7, in particular by Article 6(2) TEU, in which the Union undertakes to respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and as they derive from the constitutional traditions common to the Member States. Not only are fundamental rights, and in particular the ECHR, binding on the Member States, but the Union is also required to comply with fundamental rights in its legislation and administration. However, since at EU level there are still no regulations concerning the admissibility of the interception of telecommunications for security or intelligence purposes,⁹⁰ the issue of infringement of Article 6(2) TEU does not yet arise.

If a Member State were to promote the use of an interception system, which was also used for industrial espionage, by allowing its own intelligence service to operate such a system or by giving foreign intelligence services access to its territory for this purpose, it would undoubtedly constitute a breach of EC law. Under Article 10 TEC, the Member States are committed to acting in good faith and, in particular, from abstaining from any measure which could jeopardize the attainment of the objectives of the Treaty. Even if the interception of telecommunications is not carried out for the benefit of the domestic industry (which would, in fact, be equivalent in effect to State aid, and thus in breach of Article 87 TEC), but for the benefit of a non-member state, activities of this kind would be fundamentally at odds with the concept of a common market underpinning the EC Treaty, as it would amount to a distortion of competition.

This follows not only from the wording of the regulation as regards its scope, but also from the sense of the law. If intelligence services use their capability to gather competitive intelligence, these activities are not being carried out for the purposes of security or law enforcement but for other purposes and would consequently fall fully within the scope of the directive. Article 5 of the directive requires the Member States to ensure the confidentiality of communications. "In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users." Pursuant to Article 14, exceptions may be made only where they are necessary to safeguard national security, defense and law enforcement. As industrial espionage is no justification for an exception, it would, in this case, constitute an infringement of Community law.

To sum up, it can therefore be said that the current legal position is that in principle an ECHELON type intelligence system is not in breach of Union law because it does not concern the aspects of Union law that would be required for there to be incompatibility. However, this applies only where the system is actually used exclusively for

the purposes of state security in the broad sense. On the other hand, were it to be used for other purposes and for industrial espionage directed against foreign firms, this would constitute an infringement of EC law. Were a Member State to be involved in such action, it would be in breach of Community law. Convention on mutual assistance in criminal matters between the Member States of the European Union (OJ 2000 C 197/1, Art. 17), which regulates the conditions under which mutual assistance in criminal matters with regard to telecommunications interception is possible. These provisions in no way curtail the rights of the subjects of tapping as the Member State in which the subject is to be found has the right to refuse mutual assistance if it is not authorized under national law.

The Compatibility of Communications Surveillance by Intelligence Services With the Fundamental Right to Privacy

Any act involving the interception of communications, and even the recording of data by intelligence services for that purpose,⁹¹ represents a serious violation of an individual's privacy. Only in a "police state" is the unrestricted interception of communications permitted by government authorities. In contrast, in the EU Member States, which are mature democracies, the need for state bodies, and thus also intelligence services, to respect individuals' privacy is unchallenged and is generally enshrined in national constitutions. Privacy thus enjoys special protection: potential violations are authorized only following analysis of the legal considerations and in accordance with the principle of proportionality.

The UKUSA states are also well aware of the problem. However, these states' protection provisions are geared to respect for the privacy of their own inhabitants, so that as a rule European citizens do not benefit from them in any way. For example, the US provisions which lay down the conditions governing electronic surveillance do not set the state's interest in operating a properly functioning intelligence service against the interests

of effective, general protection fundamental rights, but rather against the need to protect the privacy of “US persons.”⁹²

Many agreements under international law specify respect for privacy as a fundamental right.⁹³ At world level, particular mention should be made of the International Covenant on Civil and Political Rights,⁹⁴ which was adopted by the UN in 1966. Article 17 of the Covenant guarantees the protection of privacy. In connection with complaints submitted by other states, all the UKUSA states have complied with the decisions taken by the Human Rights Committee set up pursuant to Article 41 of the Covenant to rule on breaches of the Covenant under international law. The Optional Protocol,⁹⁵ which extends the powers of the Human Rights Committee to cover complaints submitted by private individuals, has not been signed by the USA, however, so that such individuals cannot appeal to the Human Rights Committee in the event of the violation of the Covenant by the USA.

At EU level, efforts have been made to establish specifically European arrangements for the protection of fundamental rights through the drafting of a Charter of Fundamental Rights of the EU. Article 7 of the Charter, entitled “Respect for private and family life,” even lays down explicitly in law the right to respect for communications.⁹⁶ In addition, Article 8 lays down in law the fundamental right to the “protection of personal data.” This would have protected individuals in those cases involving the (computerized or non-computerized) processing of their data, something, which generally occurs when voice communications are intercepted and invariably does when other forms of communication are intercepted.

The Charter has not yet been incorporated into the Treaty. It is binding, therefore, only on the three institutions which pledged to comply with it in the Formal Declaration adopted during the Nice European Council: the Council, the Commission and the European Parliament. They are not involved in any secret service activities. Even

when the Charter acquires full legal force through its incorporation into the Treaty, due account will have to be taken of its limited scope. Pursuant to Article 51, the Charter applies to “the institutions and bodies of the Union—and to the Member State only when they are implementing Union law.” Accordingly, the Charter would at best take effect via the ban on state aid schemes, which run counter to the principles of competition. The only effective international instrument for the comprehensive protection of privacy is the ECHR.

The protection of fundamental rights provided by the ECHR is particularly important in that the Convention has been ratified by all the EU Member States, thereby creating a uniform level of protection in Europe. The contracting parties have given an undertaking under international law to guarantee the rights enshrined in the ECHR and have declared that they will comply with the judgments of the European Court of Human Rights in Strasbourg.

The relevant national legal provisions can thus be reviewed by the European Court of Human Rights as to their conformity with the ECHR and, in the event of a breach of human rights, a judgment may be handed down against the contracting party concerned and it may be required to pay compensation. The ECHR has gained further in importance by being repeatedly invoked by the CJEC [Court of Justice of the European Communities], alongside the general legal principles adhered to by the Member States, when that body takes decisions in cases involving legal reviews. Moreover, following the adoption of the Treaty of Amsterdam Article 6(2) of the Treaty on European Union commits the EU to respecting fundamental rights as enshrined in the ECHR.

The rights enshrined in the ECHR represent generally recognized human rights and are thus not linked to nationality. They must be granted to all persons covered by the jurisdiction of the contracting parties. In other words, the human rights in question must at all events be guaranteed throughout the territory of the contracting parties, so that local exceptions would represent a breach

of the Convention. In addition, however, they are also valid outside the territory of the contracting parties, provided that state authority is exercised in such places. Persons outside the territory of that state thus also enjoy the rights guaranteed by the ECHR vis-à-vis a contracting state if those persons suffer interference in the exercise of their right to privacy.⁹⁷

The latter point is particularly important here, since a specific characteristic of the issue of fundamental rights in the area of telecommunications surveillance is the fact that there may be a substantial geographical distance between the state responsible for the surveillance, the person under surveillance and the location in which interception is actually carried out. This applies in particular to international communications, but may also apply to national communications if information is transmitted via connections situated abroad. Indeed, this is typical of interceptions carried out by foreign intelligence services. It is also possible that information obtained by an intelligence service by means of surveillance will be passed on to other states.

Pursuant to Article 8(1) of the ECHR, “everyone has the right to respect for his private and family life, his home and his correspondence.” No explicit reference is made to the protection of telephony or telecommunications, but under the terms of the case law of the European Court of Human Rights, they are protected by the provisions of Article 8, since they are covered by the concepts of “private life” and “correspondence.”⁹⁸ The scope of the protection of this fundamental right covers not only the substance of the communication, but also the act of recording external data. In other words, even if the intelligence service merely records data such as the time and duration of calls and the numbers dialed, this represents a violation of privacy.⁹⁹

Pursuant to Article 8(2) of the ECHR, exercise of this fundamental right is not unrestricted. Interference in the exercise of the fundamental right to privacy may be admissible if there is a legal basis under national law.¹⁰⁰ The law must be generally accessible and its consequences must be foreseeable.¹⁰¹

In that connection, the Member States are not free to interfere in the exercise of this fundamental right as they see fit. They may do so only for the purposes listed in the second paragraph of Article 8 of the ECHR, in particular in the interests of national security, public safety or the economic well-being of the country.¹⁰² However, this does not justify industrial espionage, since it only covers forms of interference “necessary in a democratic society.” In connection with any instance of interference, the least invasive means appropriate must be employed to achieve the objective; in addition, adequate guarantees must be laid down to prevent misuse of this power.

These general principles have the following implications for the organization of the work of intelligence services in a manner consistent with this basic right: if, for the purpose of safeguarding national security, there seems to be a need to authorize intelligence services to record the substance of telecommunications, or at least external data relating to the connections in question, this power must be established in national law and the relevant provisions must be generally accessible. The consequences for individuals must be foreseeable, but due account must be taken of the particular requirements in the sphere of national security.

Accordingly, in a ruling on the conformity with Article 8 of secret checks on employees in areas relating to national security, the European Court of Human Rights noted that in this special case the arrangements governing the foreseeable requirement must differ from those in other areas.¹⁰³

In this context as well, however, it stipulated that the law must at all events state under what circumstances and subject to what conditions the state may carry out secret, and thus potentially dangerous, interference in the exercise of the right to privacy.¹⁰⁴ In connection with the organization of the activities of intelligence services in a manner consistent with human rights, due account must be taken of the fact that, although national security can be invoked to justify an invasion of privacy, the principle of proportionality, as defined in Article

8(2) of the ECHR, also applies: national security represents valid grounds only in cases where action to protect it is necessary in a democratic society.

In that connection, the European Court of Human Rights has clearly stated that the interest of the state in protecting its national security must be weighed up against the seriousness of the invasion of an individual's privacy.¹⁰⁵ Invasions of privacy may not be restricted to the absolute minimum, but mere usefulness or desirability is not sufficient justification.¹⁰⁶ The view that the interception of all telecommunications, even if permissible under national law, represents the best form of protection against organized crime would amount to a breach of Article 8 of the ECHR.

In addition, given the specific nature of the activities conducted by intelligence services, activities, which demand secrecy and, therefore, a particularly careful weighing-up of interests, provision must be made for more stringent monitoring arrangements. The European Court of Human Rights has explicitly drawn attention to the fact that a secret surveillance system operated for the purpose of protecting national security carries with it the risk that, under the pretext of defending democracy, it may undermine or even destroy the democratic system, so that more appropriate and more effective guarantees are needed to prevent such misuse of powers.¹⁰⁷ Accordingly, the legally authorized activities of intelligence services are only consistent with fundamental rights if the ECHR contracting party has established adequate systems of checks and other guarantees to prevent the misuse of powers.

In connection with the activities of Sweden's intelligence services, the European Court of Human Rights emphasized the fact that it attaches particular importance to the presence of MPs in police supervisory bodies and to supervision by the Minister of Justice, the parliamentary Ombudsman and the parliamentary Committee on Legal Affairs. Against this background, it must be regarded as unsatisfactory that France, Greece, Ireland, Luxembourg and Spain have no parliamentary committee with responsibility for monitoring

the secret services¹⁰⁸ and have made no move to set up a supervisory system similar to the office of parliamentary Ombudsman pioneered by the Nordic states.¹⁰⁹ Your reporter therefore welcomes the efforts made by the French National Assembly Committee on National Defense to set up a monitoring committee,¹¹⁰ particularly as France has exceptional intelligence capabilities, in both technical and geographical terms.

The contracting parties must comply with a set of conditions in order to demonstrate that the activities of their intelligence services are compatible with Article 8 of the ECHR. It is quite obvious that intelligence services cannot be allowed to circumvent these requirements by employing assistance from other intelligence services subject to less stringent rules. Otherwise, the principle of legality, with its twin components of accessibility and foreseeable would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

The first implication of this is that exchanges of data between intelligence services are permissible only on a restricted basis. An intelligence service may seek from one of its counterparts only data obtained in a manner consistent with the conditions laid down in its own national law. The geographical scope for action laid down by law in respect of the intelligence service concerned may not be extended by means of agreements with other services. By the same token, it may carry out operations on behalf of another country's intelligence service, in accordance with the latter's instructions, only if it is satisfied that the operations are consistent with the national law of its own country.

Even if the information is intended for another country, this in no way alters the fact that an invasion of privacy which could not be foreseen by the legal subject concerned constitutes a violation of fundamental rights. The second implication is that states which are ECHR contracting parties may not allow other countries' intelligence services to carry out operations on their territory if they have reason to believe that those operations are not consistent with the conditions laid down by the ECHR.¹¹¹

By ratifying the ECHR the contracting parties undertook to subject the exercise of their sovereignty to a review of its consistency with fundamental rights. They cannot seek to circumvent this requirement by foregoing the exercise of that sovereignty. These states remain responsible for their territory and thus have an obligation to European legal subjects if the exercise of sovereignty is usurped by the activities of the intelligence services of another state.

The established case law of the European Court of Human Rights now emphasizes that the contracting parties have a duty to take positive measures to protect privacy, in order to ensure that private individuals do not violate Article 8 of the ECHR. In other words, they must take action even at a horizontal level, where private individuals are not confronted with the actions of the state, but rather of other private individuals.¹¹²

If a state allows another country's intelligence service to work on its territory, the protection requirement is much greater, because in that case another authority is exercising its sovereignty. The only logical conclusion is that states must carry out checks to ensure that the activities of intelligence services on their territory do not represent a violation of human rights.

In Bad Aibling in Germany an area of land has been declared US territory for the sole purpose of housing a satellite receiving facility. In Menwith Hill in the United Kingdom authorization has been given for the shared use of land for the same purpose. If, in these stations, a US intelligence service were to engage in the interception of non-military communications conducted by private individuals or firms from an ECHR contracting party, supervisory requirements would come into play under the ECHR. In practical terms, as ECHR contracting parties Germany and the United Kingdom are required to establish that the activities of the American intelligence services do not represent a violation of fundamental rights. This is all the more relevant because representatives of NGOs and the press have repeatedly expressed

concerns regarding the activities of the US National Security Agency (NSA).

According to information available to the committee, in Morwenstow in the United Kingdom GCHQ, working in cooperation with the NSA and in strict accordance with the latter's instructions, intercepts civilian communications and passes on the recordings to the USA as raw intelligence material. The requirement to check that interception operations are consistent with fundamental rights also applies to work carried out on behalf of third parties.

In the case of operations involving two ECHR contracting parties, both can assume, up to a certain point, that the other is complying with the ECHR. At all events, this applies until evidence emerges that an ECHR contracting party is violating the Convention on a systematic, long-term basis. Things are very different, however, in the case of the USA: it is not an ECHR contracting party and it has not made its intelligence operations subject to a similar supervisory system. There are very precise rules governing the activities of its intelligence services, in so far as those activities concern US citizens or persons legally present on US territory. However, other rules apply to the activities of the NSA abroad, and many of the relevant rules are classified and thus inaccessible to the public. A further fact gives greater cause for concern, namely that although the US intelligence service is subject to monitoring by the relevant House of Representatives and Senate committees, these committees show little interest in the activities of the NSA abroad.

There would seem to be good reason, therefore, to call on Germany and the United Kingdom to take their obligations under the ECHR seriously and to make the authorization of further intelligence activities by the NSA on their territory contingent on compliance with the ECHR. In this connection, three main factors must be considered.

1. Under the terms of the ECHR, interference in the exercise of the right to privacy may

only be carried out on the basis of legal rules which are generally accessible and whose implications for individuals are foreseeable. This requirement can be met only if the USA discloses to the public in Europe how and under what circumstances intelligence gathering is carried out. If incompatibilities with the ECHR emerge, US rules must be brought into line with the level of protection provided in Europe.

2. Under the terms of the ECHR, interference in the exercise of the right to privacy must be proportional and, in addition, the least invasive methods must be chosen. As far as European citizens are concerned, an operation constituting interference carried out by a European intelligence service must be regarded as less serious than one conducted by a US intelligence service, since only in the first instance is legal redress available in the national courts.¹¹³ Operations constituting interference must therefore be carried out, as far as possible, by the German or UK authorities, particularly when investigations are being conducted for law enforcement purposes. The US authorities have repeatedly tried to justify the interception of telecommunications by accusing the European authorities of corruption and taking bribes.¹¹⁴ It should be pointed out to the Americans that all EU Member States have properly functioning criminal justice systems. If there is evidence that crimes have been committed, the USA must leave the task of law enforcement to the host countries. If there is no such evidence, surveillance must be regarded as unproportional, a violation of human rights and thus inadmissible. In other words, compliance with the ECHR can be guaranteed only if the USA restricts itself to surveillance measures conducted for the purpose of safeguarding its national security, but not for law enforcement purposes.
3. As already outlined above, in its case law the European Court of Human Rights has stipulated that compliance with fundamental rights is contingent on the existence of adequate monitoring systems and guarantees against abuse. This implies that US telecommunications surveillance operations

carried out on European territory are consistent with human rights only if the USA introduces appropriate, effective checks on such operations carried out for the purpose of safeguarding its national security or if the NSA makes its operations on European territory subject to the authority of the control bodies set up by the host state, i.e. Germany or the United Kingdom.

The conformity of US telecommunications interception operations with the ECHR can only be guaranteed and the uniform level of protection provided in Europe by the ECHR can only be maintained if the requirements set out in the three points above are met.

Although the activities of intelligence services may be covered by the CFSP [Treaty on European Union] in future, as yet no relevant rules have been drawn up at EU level, so that any arrangements to protect citizens against the activities of intelligence services can only be made under national legal systems. In this connection, the national parliaments have a dual role to play: as legislators, they take decisions on the nature and powers of the intelligence services and the arrangements for monitoring their activities.

When dealing with the issue of the admissibility of telecommunications surveillance, the national parliaments must work on the basis of the restrictions laid down in Article 8 of the ECHR, i.e. the relevant legal rules must be necessary and proportional and their implications for individuals must be foreseeable. In addition, adequate and effective monitoring arrangements must be introduced commensurate with the powers of the intelligence agencies.

Moreover, in most states the national parliament plays an active role as the monitoring authority, given that, alongside the adoption of legislation, scrutiny of the executive, and thus also the intelligence services, is the second time-honored function of a parliament. However, the Member State parliaments carry out this task in a very wide variety of differing ways, often on the basis

of cooperation between parliamentary and non-parliamentary bodies.

As a rule, the state may carry out surveillance measures for the purposes of enforcing the law, maintaining domestic order and safeguarding national security (*vis-à-vis* foreign intervention).¹¹⁵ In all Member States, the principle of telecommunications secrecy may be breached for law enforcement purposes, provided that there is sufficient evidence that a crime (possibly one perpetrated under particularly aggravating circumstances) has been committed by a specific person.

In view of the seriousness of the interference in the exercise of the right to privacy, a warrant is generally required for such an action¹¹⁶ it lays down precise details concerning the permissible duration of the surveillance, the relevant supervisory measures and the deletion of the collected data. For the purposes of guaranteeing national security and order, the state's right to obtain information is extended beyond the scope of individual investigations prompted by firm evidence that a crime has been committed.

National law authorizes the state to carry out additional measures to secure information about specific persons or groups with a view to the early detection of extremist or subversive movements, terrorism and organized crime. The relevant data is collected and analyzed by specific domestic intelligence services. Finally, a substantial proportion of surveillance measures is carried out for the purposes of safeguarding state security. As a rule, responsibility for processing, analyzing and presenting relevant information about foreign individuals or countries lies with the state's own foreign intelligence service.

In general the surveillance targets are not specific persons, but rather set areas or radio frequencies. Depending on the resources and legal powers of the foreign intelligence service concerned, surveillance operations may cover a wide spectrum, ranging from purely military surveillance of short-wave radio transmissions to the surveillance of all foreign

telecommunications links. In some Member States the surveillance of telecommunications for purely intelligence purposes is simply prohibited¹¹⁷ in other Member States—in some cases subject to authorization by an independent commission¹¹⁸—it is carried out on the basis of a ministerial order,¹¹⁹ possibly even without restriction in the case of some communication media.¹²⁰ The relatively broad powers enjoyed by some foreign intelligence services can be explained by the fact that their operations are targeted on the surveillance of foreign communications and thus only concern a small proportion of their own legal subjects, hence the substantially concern regarding lesser degree of misuse of their powers.

Effective and comprehensive monitoring is particularly important for two reasons: firstly, because intelligence services work in secret and on a long-term basis, so that the persons concerned often learn that they were surveillance targets only long after the event or, depending on the legal situation, not at all; and, secondly, because surveillance measures often target broad, vaguely defined groups of persons, so that the state can very quickly obtain a very large volume of personal data.

Irrespective of the form they take, all monitoring bodies naturally face the same problem: given the very nature of secret services, it is often extremely difficult to determine whether all the requisite information has in fact been provided, or whether some details are being held back. The relevant rules must therefore be framed all the more carefully. As a matter of principle, the effectiveness of the monitoring can be said to be high, and far-reaching guarantees that the interference is consistent with the law can be said to exist, if the power to order telecommunications surveillance is reserved for the highest administrative authorities, if the surveillance can be implemented only on the basis of a warrant issued by a judge and if an independent body scrutinizes the performance of the surveillance measures. In addition, on democratic and constitutional grounds it is desirable that the work of the intelligence service as a whole should be subject to monitoring

by a parliamentary body, in accordance with the principle of the division of powers.

In Germany, these conditions have largely been met. The responsible federal minister orders telecommunications surveillance measures at national level. Unless there is a risk that further delay may frustrate the operation, prior to the implementation of surveillance measures an independent commission not bound by government instructions (G10 Commission¹²¹) must be notified so that it can rule on the need for and the admissibility of the proposed measure. In those cases in which the German Federal Intelligence Service, FIS, can be authorized to carry out surveillance of non-cable telecommunications traffic with the aid of filtering on the basis of search terms, the Commission rules on the admissibility of the search terms as well. The G10 Commission is also responsible for checking that the persons under surveillance are notified, as required by the law, and that the FIS destroys the collected data.

Alongside this, there is a parliamentary monitoring body (PMB),¹²² which comprises nine Members of the Bundestag and scrutinizes the activities of all three German intelligence services. The PMB has the right to inspect documents, to take evidence from intelligence service staff, to visit the premises of the services and to have information notified to it; this last right can be denied only on compelling grounds concerning access to information, if it is necessary to protect the right of privacy of third parties, or if the core area of government responsibility is concerned. The proceedings of the PMB are secret and its members are required to maintain confidentiality even after they have left office. At the halfway point and at the end of the parliamentary term, the PMB submits to the German Bundestag a report on its monitoring activities.

It must be said, however, that comprehensive, monitoring of intelligence services is the exception in the Member States. In France ¹²³ for example, only those surveillance measures entailing the tapping of a cable require the authorization of the

Prime Minister. Only measures of that kind are subject to monitoring by the Commission set up for that purpose (National Commission for the Monitoring of Security-related Interceptions), whose members include an MP and a Senator. Applications for authorization to carry out an interception operation are submitted by a minister or his or her representative to the chairman of the Commission, who, if the lawfulness of the proposed operation is in doubt, may convene a meeting of the Commission, which issues recommendations and, if there are grounds for suspecting a breach of the criminal law, informs the state prosecutor's office. Measures carried out in defense of national interests, which entail the interception of radio transmissions, and thus also satellite communications, are not subject to any restrictions, including monitoring by a commission. Moreover, the work of the French intelligence services is not subject to scrutiny by a parliamentary monitoring committee; however, moves are afoot to set up such a committee. The Defense Committee of the National Assembly has already approved such a proposal¹²⁴ but no discussion of that proposal has yet taken place in plenary.

In the United Kingdom, every communications surveillance measure carried out on British soil requires the authorization of the Home Secretary. However, the wording of the law does not make it clear whether the non-targeted interception of communications, communications, which are then checked using keywords, would also be covered by the concept of 'interception' as defined in the Regulation of Investigatory Powers Act 2000 (RIP) if the intercepted communications were not analyzed on British soil, but merely transmitted abroad as 'raw material'. Commissioners—sitting or retired senior judges appointed by the Prime Minister carry out checks on compliance with the provisions of the RIP on an ex-post facto basis. The Interception Commissioner monitors the granting of interception authorizations and supports investigations into complaints concerning interception measures. The Intelligence Service Commissioner monitors the authorizations granted

for the activities of the intelligence and security services and supports investigations into complaints concerning those services.

The Investigatory Powers Tribunal, which is chaired by a senior judge, investigates all complaints concerning interception measures and the activities of the services referred to above. Parliamentary scrutiny is carried out by the Intelligence and Security Committee (ISC),¹²⁵ which monitors the activities of all three civilian intelligence services (MI5, MI6 and GCHQ). In particular, it is responsible for scrutinizing the expenditure and administration and monitoring the activities of the security service, the intelligence service and GCHQ. The committee comprises nine members drawn from the two Houses of Parliament; ministers may not be members. Unlike the monitoring committees set up by other states, which are generally elected by the national parliament or appointed by the Speaker of that parliament, they are appointed by the Prime Minister after consulting the Leader of the Opposition.

These examples already demonstrate clearly that the level of protection varies very substantially. As far as parliamentary scrutiny is concerned, the existence of a monitoring committee responsible for scrutinizing the activities of intelligence services is very important: in contrast to the normal parliamentary committees, they have the advantage of enjoying a higher degree of trust among the intelligence services, given that their members are bound by the confidentiality rule and committee meetings are held in camera. In addition, with a view to the performance of their special task they are endowed with special rights vital to the monitoring of activities in the intelligence sector. Most of the EU Member States have set up a separate parliamentary monitoring committee to scrutinize the activities of the intelligence services. In Belgium,¹²⁶ Denmark,¹²⁷ Germany,¹²⁸ Italy,¹²⁹ the Netherlands,¹³⁰ and Portugal,¹³¹ there is a parliamentary monitoring committee responsible for scrutinizing both the military and civilian intelligence service. In the United Kingdom¹³² the special monitoring committee scrutinizes only

the admittedly much more significant activities of the civilian intelligence services; the military intelligence service is monitored by the normal defense committee.

In Austria¹³³ the two arms of the intelligence service are dealt with by two separate monitoring committees, which are, however, organized in the same way and endowed with the same rights. In the Nordic states Finland¹³⁴ and Sweden¹³⁵ parliamentary scrutiny is carried out by Ombudsmen, who are independent and elected by parliament. France, Greece, Ireland, Luxembourg and Spain have no special parliamentary committees; in these countries, the standing committees, as part of their general parliamentary work, carry out monitoring tasks.

The situation for European citizens in Europe is unsatisfactory. The powers of national intelligence services in the sphere of telecommunications surveillance differ very substantially in scope, and the same applies to the powers of the monitoring committees. Not all those Member States, which operate an intelligence service, have also set up independent parliamentary monitoring bodies endowed with the appropriate supervisory powers. A uniform level of protection is still a distant objective.

From a European point of view, this is all the more regrettable, because this state of affairs does not primarily affect the citizens of the Member States concerned, who can influence the level of protection by means of their voting behavior in elections. Nationals of other states feel the adverse impact above all since foreign intelligence services, by their very nature, carry out their work abroad. Individuals are essentially at the mercy of foreign systems, and here the need for protection is greater still. It must also be borne in mind that, by virtue of the specific nature of intelligence services, EU citizens may be affected by the activities of several such services at the same time. In this context, a uniform level of protection consistent with democratic principles would be desirable. Consideration should also be given to the issue of

whether data protection provisions in this sphere would be workable at EU level.

Moreover, the issue of the protection of European citizens will be placed in an entirely new context when, under a common security policy, the first moves are made towards cooperation among the Member States' intelligence services. Citizens will then look to the European institutions to adopt adequate protection provisions. The European Parliament, as an advocate of constitutional principles, will then have the task of lobbying for the powers it needs, as a democratically elected body, to carry out appropriate monitoring. In this connection, the European Parliament will also be required to establish conditions under which the confidential processing of sensitive data of this kind and other secret documents by a special committee whose members are bound by a duty of discretion can be guaranteed. Only once these conditions have been met will it be realistic, and, with a view to effective cooperation among intelligence services to press for these monitoring rights.

Protection Against Industrial Espionage

The information held by firms falls into three categories as far as the need for secrecy is concerned. Firstly, there is information, which is deliberately disseminated as widely as possible. This includes technical information about a firm's products (e.g. specifications, prices, etc.) and promotional information which has a bearing on a firm's image. Secondly, there is information, which is neither protected nor actively disseminated, because it has no bearing on a firm's competitive position. Examples include the date of the works outing, the menu in the works canteen or the make of fax machine used by a firm. Finally, there is information, which is protected against third parties. The information is protected against competitors, but also, if a firm intends to break the law (tax provisions, embargo rules, etc.), against the state. There are various degrees of protection, culminating in strict secrecy, e.g. in the case of research findings prior to the registration of a patent or armaments production.¹³⁶ In the case under discussion here, espionage involves

obtaining information kept secret by a firm. If the assailant is a rival firm, the term used is competitive intelligence. If the assailant is a state intelligence service, the relevant term is industrial espionage.

Strategic information relevant to espionage against firms can be classified according to sectors of the economy or the departments of individual firms. It is perfectly obvious that information in the following sectors is of particular interest: biotechnology, genetic technology, medical technology, environmental technology, high-performance computers, software, opto-electronics, image sensing and signaling systems, data storage systems, industrial ceramics, high-performance alloys and nano-technology. The list is not comprehensive and changes constantly in line with technological developments. In these sectors of industry, espionage primarily involves stealing research findings or details of special production techniques.

The following departments are logical espionage targets: research and development, procurement, personnel, production, distribution, sales, marketing, product lines and finance. The significance and value of such information is often underestimated.

The strategic position of a firm on the market depends on its capabilities in the following spheres: research and development, production procedures, product lines, funding, marketing, sales, distribution, procurement and personnel.¹³⁷ Information on these capabilities is of major interest to any of the firm's competitors, since it gives an insight into the firm's plans and weaknesses and enables rivals to take strategic countermeasures.

Some of this information is publicly available. There are highly specialized consultants, including such respected firms as Roland & Berger in Germany, which draw up, on an entirely legal basis, analyses of the competitive position on a given market. In the USA competitive intelligence has now become a standard management tool. Professional analysis can turn a wide range of

individual items of information into a clear picture of the situation as a whole.

The transition from legality to a criminal act of competitive intelligence is bound up with the choice of means used to obtain information. Only if the means employed are illegal under the laws of the country concerned do efforts to obtain information become a criminal act—the provision of analyses is not in itself punishable under the law. Naturally enough, information of particular interest to competitors is protected and can only be obtained by criminal means. The techniques employed for this purpose are in no way different from general espionage methods.

No precise details are available concerning the scale of competitive intelligence operations. As in the case of conventional espionage, the official figures represent only the tip of the iceberg. Both parties concerned (perpetrator and victim) are keen to avoid publicity. Espionage is always damaging to the image of the firms concerned and the assailants naturally have no interest in public light being shed on their activities. For that reason, very few cases come to court. Nevertheless, reports dealing with competitive intelligence repeatedly appear in the press. The conclusion to be drawn is that cases of competitive intelligence repeatedly come to light, but do not determine firms' day-to-day behavior.

In view of the high number of unrecorded cases, it is difficult to determine precisely the extent of the damage caused by competitive intelligence/ industrial espionage. In addition, some of the figures quoted are inflated because of vested interests. Security firms and counterintelligence services have an understandable interest in putting the losses at the high end of the realistically possible scale. Despite this, the figures do give some idea of the problem.

As early as 1988, the Max Planck Institute estimated that the damage caused by industrial espionage in Germany amounted to at least DM 8 billion.¹³⁸ The chairman of the association of security consultants in Germany, Klaus-Dieter Matschke, quotes a figure

of DM 15 bn a year, based on expert evidence. The President of the European police trade unions, Hermann Lutz, puts the damage at DM 20 bn a year. According to the FBI,¹³⁹ US industry suffered losses of US\$ 1.7 bn as a result of competitive intelligence and industrial espionage in the year's 1992/1993. The former chairman of the Secret Service monitoring committee of the House of Representatives in the USA has spoken of losses of US\$ 100 bn sustained through lost contracts and additional research and development costs. It is claimed that between 1990 and 1996 this resulted in the loss of 6 million jobs.¹⁴⁰

Basically the exact scale of the losses is irrelevant. The state has an obligation to combat competitive intelligence and industrial espionage using the police and counterintelligence services, irrespective of the level of damage to the economy. Similarly, decisions taken by firms on the protection of information and counterespionage measures cannot be based on total damage figures. Every firm has to calculate for itself the maximum possible damage as a result of the theft of information, assess the likelihood of such events occurring and compare the potential losses with the costs of security. The real problem is not the lack of accurate figures for the overall losses, the position is rather that such cost/benefit calculations are rarely carried out, except in large firms, and consequently security is disregarded.

According to a study by the auditors Ernest Young LLP,¹⁴¹ 39% of industrial espionage is carried out on behalf of competitors, 19% for clients, 9% for suppliers and 7% for secret services. Company employees carry out espionage, private espionage firms paid hackers and secret service professionals.¹⁴²

According to the literature examined, the expert evidence presented to the committee there is a consensus that the greatest risk of espionage arises from disappointed and dissatisfied employees. As employees of the firm, they have direct access to information, can be recruited for money and will spy on their employer to obtain industrial secrets for those who hire them. Major risks also arise when employees change jobs. Today it is not necessary to copy mountains of paper in order to

take important information out of the firm. Such information can be stored on diskettes unnoticed and taken to the new employer when employees change job.

The number of firms specializing in espionage is on the increase. Former members of the intelligence services sometimes work in these firms. Frequently the firms concerned also operate as security consultants and as detective agencies employed to obtain information. In general, the methods used are legal but there are also firms, which employ illegal means.

Hackers are computer specialists with the knowledge to gain access to computer networks from the outside. In the early days, hackers were computer freaks who got a kick out of breaking through the security devices of computer systems. Nowadays there are contract hackers in both the services and on the market.

Intelligence Services

Since the end of the Cold War, the focus of the intelligence services' work has shifted. International organized crime and economic data are among their new tasks.

According to information provided by the counterintelligence authorities and by the heads of security of large firms, all tried and tested intelligence service methods and instruments are used for the purposes of industrial espionage. Firms have a more open structure than military and intelligence service facilities or government entities. In connection with industrial espionage, they are therefore exposed to additional risks: the recruitment of employees is simpler, as the facilities available to industrial security services cannot be compared to those of the counter-intelligence authorities; workplace mobility means that important information can be taken around on a laptop.

The theft of laptops or the secret copying of hard disks after hotel room break-ins is thus one of the standard methods of industrial espionage; it is

easier to break into firm's computer networks than those of security-sensitive State bodies, as small and medium-sized firms in particular have much less developed security awareness and security precautions; local tapping of communications is also easier for the same reasons. Evaluation of the information gathered on these matter shows that industrial espionage is mainly carried out locally or through mobile workstations, with a few exceptions where the information sought cannot be obtained by intercepting international telecommunications networks.

After the end of the Cold War, intelligence service capacity was released and it can now be used more than before in other areas. The United States readily admits that some of its intelligence service's activities also concern industry. This includes, for example, monitoring of the observance of economic sanctions, compliance with rules on the supply of weapons and dual-use goods, developments on commodities markets and events on the international financial markets. The US services are not alone in their involvement in these spheres, nor is there any serious criticism of this.

Criticism is leveled when state intelligence services are misused to put firms within their territory at an advantage in international competition through espionage. A distinction has to be made here between two cases.¹⁴³

Highly developed industrial states can indeed gain advantage from industrial espionage. By spying on the stage of development reached in a specific sector, it is possible to take foreign trade and subsidy measures either to make domestic industry more competitive or to save subsidies. Another focus of such activities may be efforts to obtain details of particularly valuable contracts.

Some of these states are concerned to acquire technological know-how to enable their own industry to catch up without incurring development costs and license fees. The aim may also be to acquire product designs and production methods in order to be able to compete on the world market with copies produced more cheaply by virtue of

lower wages. There is evidence that the Russian intelligence services have been instructed to carry out such tasks. The Russian Federation's Law No 5 on foreign intelligence specifically mentions obtaining industrial and scientific/technical information as one of the intelligence service's tasks.

Another group of states—Iran, Iraq, Syria, Libya, North Korea, India and Pakistan—is concerned to acquire information for their national arms programs, particularly in the nuclear sector and in the area of biological and chemical weapons. A further aspect of the activities of the services of these states is the operation of front companies, which can purchase dual-use goods without raising suspicion.

The strategic monitoring of international telecommunications can produce useful information for industrial espionage purposes, but only by chance. In fact, sensitive industrial information is primarily to be found in the firms themselves, which means that industrial espionage is carried out primarily by attempting to obtain the information via employees or infiltrators or by breaking into internal computer networks. Only where sensitive data is sent outside via cable or radio (satellite) can a communications surveillance system be used for industrial espionage. This occurs systematically in the following three cases:

1. In connection with firms, which operate in three time zones, so that interim results are sent from Europe to America and then on to Asia;
2. in the case of videoconferences in multinational companies conducted by VSAT or cable;
3. when important contracts have to be negotiated locally (construction of facilities, telecommunications infrastructure, rebuilding of transport systems, etc.), and the firm's representatives have to consult their head office.

If firms fail to protect their communications in such cases, interception can provide competitors with valuable data.

There are some cases of industrial espionage and/or competitive intelligence, which have been described in the press or in the relevant literature.

Some of these sources have been analyzed and the results are summarized in the following table. Brief details are given of the persons involved, when the cases occurred, the detailed issues at stake, the objectives and the consequences. It is noticeable that sometimes a single case is reported in very different ways. One example is the Enercom case, in connection with which either the NSA, or the US Department of Commerce or the competitor, which took the photographs, is described as the "perpetrator."

Case	Who	When	What	How	Aim	Consequence	Source
Air France	DGSRE	Until 1994	Conversation Between traveling businessmen	Bus were discovered in the first class cabins of Air France aircraft—public apology by company	Obtaining information	Not stated	“Wirtschafts-spionage: Was macht eigentlich die Konkurrenz?” von Arno Schutze, 1/98
Airbus	NSA	1994	Information on an order for aircraft concluded between Airbus and the Saudi Arabian airline	Interception of faxes and telephone calls between the negotiating parties	Forwarding of info to Airbus’s American competitors- Boeing and McDonnell-Douglas	Americans won the contract (US \$6 bn)	“Antennen gedreht,” Wirtschafts-woche Nr. 46/ 9 Nov 2000
Airbus	NSA	1994	Contract with Saudi Arabia worth US\$6 bn uncovering of bribes paid by the European Airbus Consortium	Interception of faxes and telephone calls, routed via tele-communications, satellites, between Airbus Consortium and the Saudi Arabian national airline/ Government	Uncovering of bribes	McDonnell-Douglas, Airbus’ competitor, won the contract	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell
BASF	Market Manager	Not stated	Description of the process of a raw material for skin creams by BASF (cosmetics division)	Not stated	Not stated	None, because the attempt was discovered	“Nicht gerade zimperlich,” Wirtschafts-woche Nr. 43/ 16 October 1992
Federal German Ministry of Economic Affairs	CIA	1997	Information concerning high-tech products held by the Federal Ministry of Economic Affairs	Use of an agent	Obtaining information	Agent unmasked and expelled from country	“Wirtschafts-spionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98

Case	Who	When	What	How	Aim	Consequence	Source
Federal Ministry of Economic Affairs	CIA	1997	Background to the Mykonos trial in Berlin, Hermes loads concerning exports to Iran, setting up of German firms supplying high-tech products to Iran	CIA agent disguised as US Ambassador holds friendly conversations with the Head of the Department in the Federal Ministry of Economic Affairs responsible for the Arab region (particular responsibility: Iran)	Obtaining Information	Not stated Civil servant contacts the German security authorities, who inform the Americans that the CIA operations are unwelcome. CIA agent then “withdrawn”	Industrial espionage. Firms as a target for foreign intelligence services, Badem-Wurtemberg Constitutional Protection Agency, Stuttgart as at 1998
Dasa	Russian Intel Service	1996-1999	Purchase and forwarding of armaments-related documents drawn up by a Munich arms firm (according to SZ of 20.05.2000: arms firm Dasa in Ottobrunn)	2 Germans working on behalf of the Russians	Obtaining information on guided missiles, armaments systems (anti-tank and anti-aircraft missiles)	SZ.30.05.2000 “(...) Betrayal of secrets ‘not particularly serious’ from a military point of view. The court ruled that this also applied to the economic damage suffered.”	“Anmerkungen zur Sicherheitslage der deutschen Wirtschaft,” ASW: Bonn, April 2001 “Haftstrafe wegen Spionage für Russland, SZ/ 30 May 2000
Embargo	FIS	Around 1990	Resumption of exports of embargoed technology to Libya (e.g. by Siemens)	Interception of telephone calls	Uncovering illegal arms and technology transfer	No particular consequences, deliveries not prevented	“Maulwürfe in Nadelstreifen,” Andreas Foster, p 110
Enercon	Wind power expert from Oldenburg and Kentechn employee	Not stated	Wind-power plant developed by Enercon, a firm located in Aurich	Not stated	Not stated	Not stated	“Anmerkungen zur Sicherheit der deutschen Wirtschaft,” ASW: Bonn, April 2001
Enercon	NSA	Not stated	Wind wheel for electricity generation, developed by Aloys Wobben, an engineer from East Frisia	Not stated	Forwarding of technical details to Wobben’s wind wheel to a US firm	US firm patents the wind wheel before Wobben: Wobben taken to court by US lawyers (breach of patent rights)	“Aktenkrieger,” SZ, 29 March 2001

Case	Who	When	What	How	Aim	Consequence	Source
Enercon	US firm Kene-tech Wind-power	1994	Important details of a high-tech wind-powered electricity generating plant (from switch gears to sails)	Photographs	Successful patent application in the USA	Enercon abandons plans to attack the US market	“Sicherheit muss künftig zur Chefsache werden,” HB/ 29 August 1996
Enercon	Engineer W. from Oldenburg, and US firm Kene-tech	March 1994	Type E-40 wind powered electricity generator developed by Enercon	Engineer W. passes on details, Kenetech employee photographs the plant and electrical components	Kenetech: seeking evidence for later (1995) legal action vs. Enercon for breach of patent rights Enercon: industrial espionage TV news man claims ex NSA employee told him detailed info about Enercon obtained using Enercon and passed to Kenetech by USA	Not stated	“Klettern für die Konkurrenz” SZ 13 October 2000
Enercon	Kene-tech Wind-power	Before 1996	Data concerning Enercon’s wind-powered electricity generating plant	Kenetech engineers photograph the plant	Kenetech copies the plant	Enercon vindicated: legal action brought against spy: estimated loss: several hundred million DM	“Wirtschafts-spionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98.
Japanese Trade Ministry	CIA	1996	Negotiations on import quotas for US cars on the Japanese market	Hacking into computer system of the Japanese Trade Ministry	US negotiator Mickey Kantor should accept lowest offer	Kantor accepts lowest offer	“Wirtschafts-spionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98
Japanese cars	US Govt	Not stated	Negotiations on the import of Japanese luxury cars. Info on the emissions standards of Japanese cars	COMINT, no detailed information	Obtaining information	No details	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA by Duncan Campbell

Case	Who	When	What	How	Aim	Consequence	Source
Lopez	NSA	Not stated	Videoconference involving VW and Lopez	Interception from Bad Aibling	Forwarding of info to General Motors and Opel	Interception Op allegedly provided the State Prosecutor's Office with "very detailed evidence" for its investigation	Bundeswehr Captain Erich Schmidt-Eenboom, quoted in "Wenn Freunde spionieren" www.zdf.msnbc.de/nes/54637.asp?cp1=1
Lopez	Lopez and three of his staff	1992-1993	Papers and info concerning research, planning, manufacturing and purchasing (documents concerning a plant in Spain, cost info for various model ranges, project studies purchasing and saving strategies)	Collecting information	Use of General Motors documents by VW	In the wake of legal action, the firms settle out of court. In 1996, Lopex resigns as VW manager. In 1997 VW dismisses three further members of the Lopez teams, pays US \$100 m to General Motors/Opel (supposedly lawyers' fees) and over a seven-year period purchases spare parts from GM/Opel for a total of US\$ 1 billion	Industrial espionage. Firms as a target for foreign intelligence services, Baden-Wurttemberg Constitutional Protection Agency, Stuttgart as at 1998
Lopez	NSA	1993	Videoconference between Jose Ignacio Lopez and VW boss Ferdinand Piech	Videoconference recorded and forwarded to General Motors	Protection of commercial secrets held by GM in America, secrets which Lopez wished to pass on to VW (price lists, secret plans for a new car plant and a new small car)	Lopez's cover is blown, in 1998 criminal proceedings are halted in return for payment of fines. No consequences in respect of NSA	"Antennen gedreht," Wirtschafts-woche Nr 46 / 9 November 2000 "Abgehört," Berliner Zeitung, 22 January 1996 "Die Affare Lopez ist beendet." Wirtschafts-spiegel, 28 July 1998. "Wirtschafts-spionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98

Case	Who	When	What	How	Aim	Consequence	Source
Los Alamos	Israel	1988	Two employees of the Israel nuclear research program hack into the central computer of the Los Alamos nuclear weapons laboratory	Hacking	Obtaining information about new fuses for US atomic weapons	No specific consequences since the hackers fled to Israel. One is briefly held in custody in Israel, links with the Israeli Secret Service are not officially confirmed	“Maulwürfe in Nadelstreifen,” Andreas Foster, p. 137
Smuggling	FIS	1970s	Smuggling of computers into the GDR	Not stated	Uncovering of technology transfer to the Eastern Bloc	No particular consequences, deliveries not prevented	“Maulwürfe in Nadelstreifen,” Andreas Foster, p. 113
TGV	DGSE	1993	Cost calculation by Siemens Contract to supply high-speed trains to South Korea	Not stated	Lower price offer	Manufacturer of the ICE loses the contract to Alcatel-Alsthom	“Wirtschaftsspionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98
TGV	Not known	1993	Cost calculations by AEG and Siemens concerning a government contract to supply South Korea with high-speed trains	Siemens claims that the telephone and fax connections in its Seoul office are being tapped	Negotiating advantage for the Anglo-French competitor GEC Alsthom	South Korea decides in favor of GEC Alsthom, although the German offer was initially regarded as better	“Abgehört,” Berliner Zeitung, 22 January 1996
Thomson-Alcatel v Raytheon	CIA/ NSA	1994	Award to the French firm Thomson-Alcatel of a Brazilian contract for the satellite monitoring of the Amazon Basin (US\$ 1.4 bn)	Interception of communications to and from the successful tenderer Thomson-Alcatel	Uncovering corruption (payment of bribes)	Clinton complains to the Brazilian Government; under pressure from the USG, the contract is awarded to the US firm Raytheon	“Maulwürfe in Nadelstreifen,” Andreas Forster, p. 91
Thomson-Alcatel v Raytheon	US Dept of Commerce ‘made effort’	1994	Negotiations on a project worth billions of dollars concerning the radar monitoring of the Brazilian rainforest	Not stated	Win Contract	The French firms Thomson CSF and Alcatel lose the contract to the US firm Raytheon	“Antennen gedreht,” Wirtschaftswoche Nr 46 / 9 November 2000

Case	Who	When	What	How	Aim	Consequence	Source
Thomson-Alcatel v Raytheon	NSA Depart of Com- merce		Negotiations concerning a project worth US\$ 1.4 bn concerning the monitoring of Amazon Basin (SIVA) Discovery that the Brazilian selection panel had accepted bribes. Comment by Campbell: Raytheon supplies equipment for the Sugar grove interception station	Surveillance of the negotiations between Thomson-CSF and Brazil and forwarding of the findings to Raytheon Vcorp	Uncovering bribery Winning of the contract	Raytheon wins the contract	“Development of Surveillance Technology and Risk of Abuse of Economic Information,” Vol 2/5 10 1999 STOA, von Duncan Campbell
Thyssen	BP	1990	Gas and oil drilling contract in the North Sea worth millions of dollars	Interception of faxes sent by the successful tendered (Thyssen)	Uncovering corruption	BP brings an action for damages against Thyssen	“Maulwürfe in Nadelstreifen,” Andreas Forster, p. 92
VW	Not known	‘recent years’	Not stated	Inter alia, infrared camera, fixed in a mound of earth, which transmits images by radio	Obtaining information about new developments	VW admits losses of profits totalling hundreds of millions of deutschmarks	“Sicherheit muss künftig zur Chefsache werden,” HB / 29 August 1996
VW	Not known	1996	VW test circuit in Ehra-Lessien	Hidden camera	Information about new VW models	Not stated	“Auf Schritt und Tritt” Wirtschafts- woche nr 25, 11 June 1998

The legal systems of all the industrialized countries define the theft of commercial secrets as a criminal offence. As in all other areas of the criminal law, the degree of protection varies from country to country. As a rule, however, the penalties for industrial espionage are much less severe than those for espionage in connection with military security. In many cases, competitive intelligence operations are banned only against firms from the same country, but not against foreign firms abroad. This is also the case in the USA.

In essence, the relevant laws prohibit only espionage by one industrial undertaking against another. It is doubtful whether they also restrict the activities of state intelligence services, since, on the basis of the laws establishing them, the latter are authorized to steal information. A gray area develops if intelligence services seek to pass on to individual firms' information gained by means of espionage. The laws, which endow intelligence services with special powers, would normally not cover such activities. In particular, in the EU this would represent a breach of the EEC Treaty.

Irrespective of this fact, however, in practice it would be very difficult for a firm to seek legal protection by bringing an action before the courts. Interception operations leave no trace and generate no evidence, which might be used in court.

States accept the fact that intelligence services, in keeping with their general objective of securing strategic information, are also active in the commercial sphere. However, this gentlemen's agreement is frequently breached in connection with competitive intelligence operations designed to benefit a country's own industry. Any state caught red-handed comes under massive political pressure. This applies in particular to a world power such as the USA, whose claim to global political leadership would be drastically undermined. Middle-ranking powers could probably afford to be singled out for such activities; a superpower certainly cannot.

Alongside the political problems, there is also the practical issue of which individual firm is

to be provided with the information gained by means of competitive intelligence operations. In the aerospace sector, the answer is a simple one, because only two major firms dominate the global market. In all other cases where a market is supplied by a number of firms, which are not state-controlled, it is extremely difficult to give preference only to one. In connection with international contract-award procedures, an intelligence service is more likely to forward detailed information concerning other competitors' offers to all the participating firms from its own country, rather than simply to one. This applies in particular when all the participating firms from one country can draw on the same level of government support, as is the case in the USA through the work of the Advocacy Center. In the case of the theft of technology, which should necessarily lead to the registration of a patent, it is only logical that such equal treatment would no longer be possible. Moreover, under the US political system in particular this would give rise to a serious problem. US politicians are massively dependent on contributions from firms in their constituencies to finance their election campaigns. If proof were to emerge of even one case of intelligence services favoring individual firms, the upheaval in the political system would be massive. As the former CIA Director James Woolsey put it in a discussion with representatives of the committee: "In that case the Hill—i.e. the US Congress—would go mad!" Quite!

Since 1990, the US Administration has increasingly come to equate national security with economic security. The annual White House report entitled, National Security Strategy repeatedly emphasizes that economic security is fundamental not only to our national interests, but also to national security. This development can be traced back to a number of sources. Essentially, three factors came together:

1. The interest of the intelligence services in taking on a task which would outlive the Cold War;
2. The US State Department's simple acknowledgement of the fact that, following the

-
- Cold War, the USA's leading role in the world could not be based solely on military strength, but also made economic strength essential;
3. President Clinton's interest, from a domestic policy point of view, in strengthening the US economy and creating jobs.

This combination of interests had practical consequences.

As a logical response, since 1992, the FBI has focused its counterintelligence activities on industrial espionage and, in 1994, it set up an Economic Counterintelligence Program. Speaking to the US Congress, Louis J. Freeh, the Director of the FBI, described this as a defensive program designed to prevent the competitiveness of the US economy from being undermined by the theft of information.

As a logical response, at least from an American point of view, the Administration has used the CIA, and subsequently the NSA, to prevent distortions of competition by means of bribery. The former Director of the CIA, James Woolsey, made this explicitly clear at a press conference he gave on 7 March 2000 at the request of the US State Department.¹⁴⁴ As a logical response, the US Department of Commerce has focused its efforts to foster exports in such a way that a US firm wishing to export goods need only deal with one agency. Active use is made of all the weapons at the Administration's disposal.

Intelligence operations directed against the US economy are neither unusual nor new. For decades, both the USA and other leading industrialized countries have been targets for industrial espionage. During the Cold War, however, economic and technological intelligence gathering took second place to conventional espionage. Following the end of the Cold War, industrial espionage has come into its own.¹⁴⁵

In 1996, speaking to the US Congress, the Director of the FBI, Louis J. Freeh, gave a detailed account of the way the US economy has become a target for industrial espionage by other countries'

intelligence agencies. As he put it, consequently foreign governments, through a variety of means, actively target US persons, firms, industries and the US Administration itself, to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage. However, the theft of information by Americans was increasing just as much. The further remarks made by Mr. Freeh to the US Congress are summarized below.

At this point, your reporter would like to express regret at the fact that the US Administration did not allow a delegation from the Temporary Committee to discuss these issues with the FBI. Up-to-date information could then have been obtained. In the paragraphs, which follow, therefore, your reporter has assumed that the US Administration takes the view that the hearing before the House of Representatives held in 1996 gives an accurate picture of the threat currently posed to the US economy by industrial espionage. Accordingly, he has drawn extensively on that source.

At the time of the hearing, the FBI was investigating persons or organizations from 23 countries, which were suspected of industrial espionage against the USA. Some ideological or military opponents of the USA have merely continued their Cold War activities.¹⁴⁶ In contrast, other governments carry out industrial and technological espionage, even though they have long been the USA's military and political allies. In so doing, they often exploit their ease of access to US information. Some have developed agencies, which assess information concerning high-technology products and use that information in competition with US firms. No countries have actually been named, although the involvement of Russia, Israel and France has been hinted at.¹⁴⁷

High-technology products and the defense industry are given as priority objectives. Interestingly enough, the FBI names information concerning bids, contracts, clients and strategic information in these areas as objectives of industrial espionage, which are pursued aggressively.¹⁴⁸

In the context of the Economic Counterintelligence Program, the FBI has identified a series of espionage methods. A combination of methods is employed in most cases, a single method only rarely. According to the information obtained by the FBI, the best source is a person employed by a firm or organization, something, which is not only true for the USA. At the hearing, the FBI outlined how persons are used to carry out for espionage, but astonishingly gave no details of electronic methods.

At a press conference¹⁴⁹ and in a conversation with members of the committee in Washington, the former Director of the CIA, James Woolsey, briefly summarized the interception activities of the US Secret Service as follows:

1. The USA monitors international telecommunications in order to obtain general information about economic developments, shipments of dual-use goods and compliance with embargoes.
2. The USA monitors on a targeted basis communications by individual firms in connection with contract-award procedures in order to prevent corruption-related distortions of competition to the detriment of US firms. Questioned more closely, however, Woolsey gave no specific examples.

US firms are banned by law from paying bribes and accountants are required to report evidence of such payments. If a telecommunications surveillance operation reveals evidence of bribery in connection with public contracts, the US ambassador makes representations to the government of the country concerned. However, US firms competing for the contract are not directly informed. He categorically ruled out the possibility of espionage solely for the purposes of obtaining competitive intelligence.

At a hearing before the House Permanent Select Committee on Intelligence held on 12 April 2000, the current Director of the CIA, George J. Tenet, echoed Woolsey's comments: It is not the policy nor the practice of the United States to engage in espionage that would provide an unfair advantage

to US companies. At the same hearing, Tenet went on to say that information on the payment of bribes was forwarded to other government agencies so that they could help US firms.¹⁵⁰ In response to a supplementary question from Congressman Gibbons, Tenet admitted that there was no legal ban on the gathering of competitive intelligence; however, he saw no need for such a ban, given that the intelligence services were not involved in activities of that kind. In the course of a conversation held with him in Washington, the chairman of the House Permanent Select Committee on Intelligence, Porter Goss, painted a similar picture of US interception activities.

Legal Situation With Regard to the Payment of Bribes to Public Officials¹⁵¹

The payment of bribes to secure contracts is a worldwide, and not simply European, phenomenon. According to the Bribe Payers Index (BPI) published by Transparency International in 1999, which ranks the 19 leading exporting countries on the basis of their willingness to offer bribes, Germany and the USA share ninth place. Sweden, Austria, The Netherlands, the United Kingdom and Belgium were identified as being less likely to offer bribes; only Spain, France and Italy have a higher rating.¹⁵²

The Americans refer to the corrupt practices employed by European firms to justify industrial espionage. This is questionable, not only because wrongdoings by individual firms cannot justify the comprehensive use of espionage. Such heavy-handed practices could only be tolerated if there were a legal vacuum in this area.

However, the legal measures taken to combat corruption are just as stringent in Europe as they are in the USA. In 1997, these shared interests led to the adoption of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The Convention requires the signatory states to make the payment of bribes to a foreign public official a criminal offence and contains, alongside a definition of the offence of bribery, provisions concerning penalties, jurisdiction and enforcement.

The Convention, which came into force on 15 February 1999, has been transposed and ratified by all the EU Member States except Ireland. The USA transposed the Convention by adopting the 1998 International Anti-Bribery and Fair Competition Act amending the Foreign Corrupt Practices Act (FCPA) of 1977, which imposes on firms a requirement to keep accounts and prohibits the payment of bribes to foreign public officials.¹⁵³ Neither in the USA nor in the EU Member States are bribes accepted as tax-deductible operating expenditure.¹⁵⁴ Whereas the OECD Convention is designed only to combat the payment of bribes to foreign public officials, in 1999 the Council of Europe adopted two more far-reaching agreements, although neither has yet come into force.

The Criminal Law Convention on Corruption¹⁵⁵ also encompasses bribery in the private sector. It was signed by all the EU Member States except Spain and by the USA, but as yet has been ratified only by Denmark. The Civil Law Convention on Corruption¹⁵⁶ lays down rules governing liability and compensation, stipulating in particular those contracts and contract clauses, which require firms to pay bribes, will be deemed null and void. All the EU Member States except the Netherlands, Portugal and Spain have signed it; the USA has not signed.

The EU has adopted two further legal acts designed to combat bribery: the Convention on the fight against corruption involving officials and the Joint Action on corruption in the private sector. The Convention on the fight against corruption involving officials of the European Communities or officials of the EU Member States¹⁵⁷ is designed to ensure that corruption and the payment of bribes to officials are criminal offences throughout the EU. The Member States undertake to make both the payment of bribes to an official and corruption criminal offenses, regardless of whether one of their own officials, an official of another Member State or an EU official is involved.

The Joint Action on corruption in the private sector¹⁵⁸ is intended to ensure that corruption and the payment of bribes to firms are criminal offences.

In that connection, criminal law penalties are laid down for both natural and legal persons. However, the scope of the Joint Action is more restricted than that of the Convention on the fight against bribery involving officials in that it requires the Member States only to punish actions carried out at least in part on their territory. Member States are free to extend this jurisdiction to cover actions carried out abroad by their own nationals or to the benefit of domestic legal persons. Germany and Austria have made instances of corruption carried out abroad criminal offences provided that they are also punishable in the country concerned.

By means of Executive Order 12870, in 1993 President Clinton set up the Trade Promotion Coordinating Committee (TPCC).¹⁵⁹ Its role is to coordinate and develop a strategy for the US Administration's trade promotion policy. In accordance with the Executive Order, a representative of the National Security Council (NSC) also sits on the TPCC.¹⁶⁰ The NSC formulates the United States' national security policy with reference to domestic policy, foreign policy, military and intelligence issues. Each president alters the focus of the NSC's work. On 21 January 1993, by means of PDD2, President Clinton expanded the NSC and, at the same time, placed more emphasis on economic issues in connection with the formulation of security policy. Members of the NSC include the President, the Vice-President, the Secretary of State and the Secretary of Defense. The Director of the CIA is an advisory member.

The Advocacy Center, which is attached to the US Department of Commerce, is at the heart of the national export strategy employed by President Clinton and continued by President Bush. It acts as the interface between the TPCC and the US economy. By its own account, since its inception in 1993 the Center has helped hundreds of US firms to win public contracts abroad. The Advocacy Center helps US businesses by:¹⁶¹

- marshalling the resources of the US Administration - from the various financing, regulatory, country and sector experts, through

the worldwide network of commercial officers, to the White House;

- fighting to level the playing field and promote open competition in the international bidding arena—from the multibillion dollar infrastructure project to the strategic contract for a small business;
- pursuing deals on behalf of US companies from start to finish, through ‘hands-on’ support;
- supporting US jobs and boosting US exports through the successes of US companies who successfully bid for overseas projects and contracts;
- assisting US firms with stalled negotiations due to foreign government inaction or “red tape.”

Only the Director and a small staff complement of 12 people work at the Advocacy Center¹⁶² itself—situation as at 6 February 2001. The project managers cover the following areas: Russia and the newly independent countries; Africa, East Asia and the Pacific; the Middle East and North Africa; South Asia—Bangladesh, India, Pakistan, Sri Lanka; Europe and Turkey; China, Hong Kong and Taiwan—Canada, the Caribbean and Latin America; the aerospace, automobile and defense industries worldwide; and the telecommunications, IT and computer industries worldwide.

The Center provides firms with a central contact point for their dealings with the various US authorities involved in promoting exports. It works on behalf of firms on a non-discriminatory basis, but, in line with the clear rules governing its work, supports only projects, which are in the US national interest. For example, projects manufactured in the USA must make up at least 50% of the value of the goods delivered under any given contract.

Duncan Campbell submitted to the members of the Temporary Committee a number of declassified documents, which provide evidence of CIA involvement in the work of the Advocacy Center. They include minutes of the Trade Promotion Coordinating Committee dealing with a meeting of the Indonesia Working Group held in July and August 1994.¹⁶³ According to the documents, a number of CIA staff members sit on the Working

Group, whose task is to draw up a trade strategy for Indonesia. The CIA staff members are named in the minutes. Moreover, the minutes show that one of the CIA staff members defines one objective of the Working Group as that of identifying main competitors and making this background information available to firms.¹⁶⁴

The US Administration did not allow the discussion arranged between members of the Temporary Committee and representatives of the Center to take place. For that reason, two areas of doubt could not be cleared up:

- the Temporary Committee has in its possession documents which provide evidence of CIA involvement in the work of the TPCC;
- in its own information brochure (quoted above), the Advocacy Center acknowledges that it focuses the resources of 19 “US government agencies.” Elsewhere in the brochure, however, only 18 such agencies are listed, raising the issue of why the 19th cannot be named in public.

Security of Computer Networks

Nowadays, alongside the use of spies, hacking into computer networks or the theft of data from laptop computers represents the second most effective method of industrial espionage. The information here has no direct bearing on the existence or otherwise of a global system for the interception of international communications. However, in view of the Temporary Committee’s aims, the chapter on industrial espionage must include brief details of one of its most powerful tools. This will certainly help readers to assess the significance of a system for the interception of international communications in connection with industrial espionage.

Modern electronic data-processing technologies have been in common use by firms for some time now. Data of all kinds is stored in highly compressed form on a variety of media. Data stored on computer has now become one of the key aspects of commercial know-how. This transition from an industrial to an information society is

opening up new opportunities, but, at the same time, creating substantial security risks.¹⁶⁵

The new risks, which are emerging, can be summarized as follows:¹⁶⁶

- More and more firms have computer networks and more and more information is being condensed in one place, with the result that it can be copied simply by hacking into the network. At the same time, other sensitive items of information are being decentralized and are thus not easily accessible in the context of a centralized security management strategy.
- The mobility of senior managers, who carry sensitive information with them on their laptop computers, is creating additional risks. The outsourcing of services is giving rise to new maintenance practices in the IT sphere as well which are highly questionable from a security point of view.
- A combination of the low status accorded to security staff in firms' management hierarchy and senior managers' ignorance of security issues is giving rise to misguided decisions.

Nowadays, firms' business secrets are stored in a physically very small area on compressed media. As a result, for example, the full plans for a new factory can be smuggled out of a firm on a substitute hard disk the size of a cigarette packet or copied electronically in minutes, without leaving any trace, by hacking into a computer network.

In the era of large-scale computers, it was easy to monitor access to secret information, since only one computer was involved. Today, each employee connected to the network is provided with substantial computing capacity at his or her workstation. This is of course a great advantage for the staff member concerned, but a disaster from a security point of view.

In the era of hand-drawn plans and mechanical typewriters it was very difficult to copy large numbers of documents without being detected. Today, in the electronic era, it is easy. Large volumes of digitized information can be copied

easily, quickly and without leaving any trace. As a result, in many cases only one intervention is needed to obtain the material in question and the risk of being detected are correspondingly much lower.

Often without being properly aware of the fact, senior managers often carry strategically important information about their firms with them on their laptop computers. The speed with which a copy of the hard disk can be made in the course of a "customs check" or a search of a hotel room offers intelligence services substantial opportunities for action. Alternatively, the Notebook in question is simply stolen. Moreover, in view of the decentralization involved it is difficult to incorporate into a central security management strategy the information stored on the hard disks of laptop computers used by a firm's senior managers.

Although outsourcing may serve to reduce a firm's costs, in the sphere of information technology and the maintenance of telephone networks it allows technicians from outside the firm virtually unrestricted access to information. The associated risks cannot be over-emphasized.

Alongside security loopholes in the software itself, which hackers repeatedly find, the most serious danger stems from network administrators who are not properly aware of the risks. In its basic form, Windows NT is configured in such a way that it reveals almost all the information required for a successful attack on the network.¹⁶⁷ If these configurations and standard passwords are not changed, accessing the network is child's play. Firms often make the mistake of investing considerable amounts of time and money in the security of the firewall, but fail to protect the network properly against attacks from within.¹⁶⁸

The number of instances of computer networks being hacked into via the Internet is increasing every year.¹⁶⁹ In 1989, the Computer Emergency Response Team (CERT), an organization set up in the USA in 1988 with the aim of improving Internet security, received notification of 132 security problems. In 1994, the figure had already

risen to 2241 and in 1996 it reached 2573. The real figure is certainly much higher. This assumption was backed up by a large-scale simulation, which the US Department of Defense carried out using its own computers. Systematic efforts were made to hack into 8932 servers and mainframe computers from outside. In 7860 cases these attempts proved successful, only 390 attempts were detected and no more than 19 cases were reported.

A distinction must be drawn between attacks and security problems. An attack is a single attempt to gain unauthorized access to a system. A security problem consists of a number of related attacks. Extrapolating from their own long-term studies, the Pentagon and US universities have posited a figure of 20000 security problems and 2 million attacks on the Internet annually.

The aim of foreign intelligence services, which attack IT systems, is to secure the information they contain, if at all possible without being detected. In principle, a distinction can be drawn between three groups of perpetrators with three different *modi operandi*.

A spy who has been smuggled into a firm or whose services have been bought and who has risen to become a systems administrator or security administrator in a computer center need only make extensive use of the powers officially granted to him in order to steal virtually all his employer's know-how. The same applies to a senior development engineer with unrestricted access authorization to all a firm's databanks. A spy of this kind offers maximum espionage effectiveness. However, if suspicions arise, the risk of detection is high, since the investigations immediately focus on the small group of persons who have comprehensive access to information. Moreover, it is pure coincidence if a spy secures comprehensive access authorization.

A spy working within a firm has a clear advantage over a hacker attacking from the outside: he must overcome only the network security precautions, but no firewall. From an individual workstation, and provided that the person concerned has

the requisite knowledge, the architecture of the network can be established and substantial volumes of information can be obtained, using the same techniques employed by an outside hacker and other techniques available only to persons working from within.¹⁷⁰ In addition, the spy can converse with colleagues without raising suspicion and obtain passwords by means of "social engineering." The effectiveness of such a spy can be high, but is not as predictable as in the first case. The risk of detection is lower, particularly in the case of networks whose administrator pays little attention to the dangers of an attack from within. It is much easier to smuggle in a spy trained to hack into computer networks (trainees, guest researchers, etc.).

That hackers repeatedly gain unauthorized access to computer networks is well known and well documented. Intelligence services themselves now train specialists in the skills needed to hack into computer networks. The effectiveness of such an attack cannot be predicted or planned; it depends to a great extent on the effectiveness of the network defense mechanisms and on whether, for example, the network used by the research department is physically linked to the Internet. The level of risk involved for a professional spy is virtually zero; even if the attack is detected, the spy is somewhere else entirely.

As things stand, awareness of the risk of industrial espionage is not very well developed in individual firms. This is partly reflected in the fact that security officers often have middle- management rank and are not board members. However, security costs money and board members generally take an interest in security issues only when it is too late. Large firms do at least have their own security departments and employ security specialists in the IT sphere as well. In contrast, small and medium-sized firms vary rarely employ security experts and are generally happy enough if their data-processing equipment works properly. However, such firms as well may be targets for industrial espionage, since many of them are highly innovative. Moreover, in view of their integration in the production process medium-

sized component suppliers offer a suitable basis for industrial espionage operations against large firms.

As a rule, researchers are interested only in their area of expertise and can therefore sometimes be an easy target for intelligence services. Your reporter has noted with some amazement that research institutes whose work has obvious practical applications communicate with each other using unencrypted e-mails and the science network. This is quite simply reckless.

Information concerning preparations for decisions by the European Central Bank (ECB) could be of great value to intelligence services—and, it goes without saying, of course to the markets. At a meeting held in camera, the committee heard statements by representatives of the ECB concerning the security precautions taken to protect information. On that basis, your reporter has come to the conclusion that the ECB is aware of the risks and, as far as is feasible, is taking appropriate security measures. However, he has been supplied with information suggesting that risk-awareness is low in certain national central banks.

Prior to the appointment of the High Representative for the common foreign and security policy, the Council focused its efforts in the area of secrecy on measures to keep information concerning decision-making procedures and the stances adopted by the Member State governments from the public and the European Parliament. It would have had no defense against a professional intelligence operation.¹⁷¹ For example, an Israeli firm apparently carried out technical maintenance in the interpreting booths. The Council has now adopted security regulations¹⁷² consistent with the standard within NATO.

Up to now, the European Parliament has never dealt with classified documents and therefore has no experience in the area of the protection of secrecy and no security culture. The need for such a culture will only arise if Parliament gains access to classified documents in the future. Otherwise, a general policy of secrecy is anathema for a parliament whose actions must be as transparent

as possible. However, with a view to protecting informants and petitioners, provision should be made for the encryption of e-mails transmitted from one Member's office to another. At present, this is not possible.

The European Commission has directorates-general, which by virtue of the information they deal with have no need for secrecy rules or protection arrangements. Indeed, the reverse is true: complete transparency should be the norm in all areas, which have a bearing on legislation. The European Parliament must employ a vigilant approach in order to ensure that, in these areas, the influence exerted on legislative proposals by interested firms, etc. is not masked even more than it already is through the unnecessary introduction of inappropriate secrecy rules.

Admittedly, there are areas of the Commission's work, which involve the processing of sensitive information. Alongside Euratom, the most obvious areas are foreign relations, foreign trade and competition. On the basis of the information supplied by the directorates-general concerned to the committee at a meeting held in camera, and above all on the basis of other information, it is very doubtful as to whether the European Commission is properly aware of the risk of espionage and whether it takes a professional approach to the issue of security. Naturally enough, a public report is no place in which to outline security shortcomings. Nevertheless, there is a pressing need for the European Parliament to consider this issue in an appropriate manner.

However, it can be stated now that the encryption systems, which the Commission employs when communicating with some of its external offices, are outdated. This does not mean that the security standard is poor. However, the equipment currently in use is no longer manufactured and only roughly half of the external offices are equipped with encryption technology. The introduction of a new system working on the basis of encrypted e-mails is an urgent necessity.

Cryptography as a Means of Self-Protection

Every time a message is transmitted, there is a risk of its falling into unauthorized hands. To prevent outsiders ascertaining its content in such cases, the message must be made impossible for them to read or intercept, i.e. encrypted. Consequently encryption techniques have been used since time immemorial for military and diplomatic purposes.¹⁷³

In the past 20 years the importance of encryption has increased, since an ever greater proportion of communications has been sent abroad, where the confidentiality of post and telecommunications could not be guaranteed by the state of origin. Moreover, the expanded technical opportunities for the state legally to intercept/record communications on its own territory has led to concern among ordinary citizens and a greater need for their protection.

Finally, the increased interest among criminals in having illegal access to information, and the ability to falsify it, has also given rise to protection measures (e.g. in the banking sector). The invention of electrical and electronic communications (telegraph, telephone, radio, telex, fax and Internet) greatly simplified the transmission of intelligence communications and made them immeasurably quicker. The downside was that there was no technical protection against interception or recording, so that anyone with the right equipment could read the communication if he could gain access to the means of communication. If done professionally, interception leaves little or no trace. This imparted a new significance to encryption. It was the banking sector, which first regularly used encryption to protect communications in the new area of electronic money transfers. The growing internationalization of the economy led to communications in this field, too, being at least partly protected by cryptography. The widespread introduction of completely unprotected communications through the Internet also increased the need for private individuals to protect their messages from interception.

In the context of this report, then, the question arises as to whether there are cheap, legal, sufficiently secure and user-friendly methods of encrypting communications, which can protect the individual against interception.

The principle of encryption is to convert a plain text into an encrypted text in such a way that it has either no meaning or a different meaning from the original, but can be converted back to the original by those in the know. For example, a meaningful sequence of letters can be transformed into a meaningless sequence, which no outsider understands. This is done according to a given method (encryption algorithm) based on the transposition and/or the substitution of letters. The encryption method (algorithm) is not nowadays kept secret. On the contrary, a worldwide invitation to tender was recently issued for a new global encryption standard for use in industry.

The same was done for the creation of a specific encryption algorithm as hardware in a machine (e.g. an encrypted fax machine). What is really secret is the key to the code. This can be best explained by analogy. It is generally public knowledge how door locks work, not least because patents are held on them. Individual doors are protected by the fact that several different keys can exist for a particular type of lock. The same goes for the encryption of information: many different messages may be protected using individual keys, kept secret by those involved, on the basis of one publicly known encryption method (algorithm).

To explain these terms, we may use the example of the Caesarean encryption. Julius Caesar encrypted messages simply by replacing each letter with the letter three places further on in the alphabet (A became D, B became E, etc.). The word ECHELON would thus become HFKHORQ. The encryption algorithm thus consists of the shifting of letters within the alphabet, and the key in this particular case is the instruction to move the letters three places in the alphabet. Both encryption and decryption are done in the same way: by moving letters three places: a symmetrical process.

Nowadays this type of process would not provide protection for as much as a second!

A good encryption system may perfectly well be publicly known and still be regarded as secure. For this purpose, however, the number of possible keys needs to be so large that it is not possible to try all the keys (known as a brute force attack) in a reasonable time, even using computers. However, a large number of possible keys do not necessarily imply secure encryption if the method results in an encrypted text which gives clues to its decryption (e.g. the frequency of particular letters).¹⁷⁴ Caesar's encryption is thus an insecure system for both reasons. Because it uses simple substitution, the varying frequency of letters in a language means that the procedure can quickly be cracked; moreover, since there are only 26 letters in the alphabet, there are only 25 possible letter shifts and thus only 25 possible keys. In this case, then, the code breaker could very quickly find the key by trying all the possibilities and decipher the text. If an encryption system is required to be secure this may mean one of two things. Either it may be essential and susceptible of mathematical proof that the message is impossible to decipher without the key. Or it may be sufficient for the code to be unbreakable at the present state of technology and thus in all probability to meet the security requirement for far longer than the critical period during which the message needs to be kept secret.

At present the only absolutely secure method is the one-time pad. This system was developed towards the end of the First World War,¹⁷⁵ but was also used later for the telex hot line between Moscow and Washington. The concept consists of a key comprising a non-repeating row of completely random letters. Both sender and recipient encrypt using these rows, and destroy the key as soon as it has been used once. Since there is no internal order within the key, it is impossible for a cryptanalyst to break the code. This can be mathematically proven.¹⁷⁶

The drawback to this process is that it is not easy to generate large numbers of these random keys,¹⁷⁷ and that it is difficult and impractical to find a secure

means of distributing the key. In normal business transactions, therefore, this method is not used.

Even before the invention of the one-time pad, cryptographic processes were developed, which could generate a large number of keys and thus produce coded texts which contained as few regularities in the text as possible and thus few starting-points for code breaking. In order to make these methods sufficiently fast for practical application, machines were developed for encryption and decryption. The most spectacular of these was probably Enigma,¹⁷⁸ used by Germany in the Second World War. The small army of decryption experts working at Bletchley Park in England succeeded in cracking the Enigma code by means of special machines known as bombs. Both the Enigma machine and the bombs were mechanical in operation.

The invention of the computer represented a breakthrough in cryptography, since its power made it possible to use increasingly complex systems. Even though it did not alter the basic principles of encryption, a number of changes took place. Firstly, the level of potential complexity of the encryption system was multiplied, since it was no longer subject to the constraints of what was mechanically feasible, and, secondly, the speed of the encryption process rose drastically. In computers, information is processed digitally using binary numbers. This means that the information is expressed by the sequence of two signals 0 and 1. In physical terms 1 corresponds to an electric current or magnetic field (light on), while 0 means the absence of current or magnetic field (light off).

ASCII¹⁷⁹ standardization now prevails, whereby each letter is represented by a seven-figure combination of 0 and 1.¹⁸⁰ A text therefore appears as a sheet of 0s and 1s, and instead of letters it is numbers that are encrypted. Both transposition and substitution can be used in this process. Substitution may, for example, take place by the addition of a key in the form of any row of numbers. According to the rules of binary mathematics the sum of two equal figures is zero ($0+0=0$ and $1+1=0$) while the sum of two different

figures is 1 ($0+1=1$). The new, encrypted row of figures arising from the addition of the key is thus a binary sequence, which can either be further digitally processed or made readable again by subtracting the added key.

The use of computers made it possible to generate coded texts, using powerful encryption algorithms, which offer practically no starting-points for code breakers. Decryption now entails trying all possible keys. The longer the key, the more likely it is that this attempt will be thwarted, even using very powerful computers, by the time it would take. There are therefore usable methods, which may be regarded as secure at the present state of technology.

As computers became more widely available in the 1970s, the need for the standardization of encryption systems grew ever more urgent, since only in this way could firms communicate securely with business partners without incurring disproportionate costs. The first moves were made in the USA. Powerful encryption systems can also be used for unlawful purposes or by potential military opponents; they may also make electronic espionage difficult or impossible. For that reason, the NSA urged that firms should be offered a sufficiently secure encryption standard, but one which the NSA itself could decrypt, by virtue of its exceptional technical capabilities. With that aim in mind, the length of the key was restricted to 56 bits. This reduces the number of possible keys to 100 000 000 000 000 000.¹⁸¹ On 23 November 1976 Horst Feistel's so-called Lucifer key was officially adopted in its 56-bit version under the name Data Encryption Standard (DES) and for the next 25 years represented the official US encryption standard.¹⁸²

This standard was also adopted in Europe and Japan, in particular in the banking sector. Media claims to the contrary, the DES algorithm has not yet been broken, but hardware now exists, which is powerful enough to try all possible keys (brute force attack). In contrast, Triple DES, which has a 112-bit key, is still regarded as secure. The successor to DES, the Advanced Encryption

Standard (AES), is a European process,¹⁸³ which was developed under the name Rijndael in Louvain, Belgium. It is fast and is regarded as secure, since it incorporates no key-length restriction. The reason for this lies in a change in US policy on cryptography. Standardization makes it much easier for firms to employ encryption. What remained, however, was the problem of key exchange.

As long as a system works with a key, which is employed both for encryption and decryption (symmetric encryption), it is difficult to use with large numbers of communication partners. The key must be handed over to every new communication partner in advance in such a way that no third party gains access to it. This is difficult for firms in practical terms, and feasible for private individuals only in rare cases.

Asymmetric encryption offers a solution to this problem: two different keys are used for encryption and decryption. The message is encrypted using a key, which may perfectly well be in the public domain, the so-called public key. However, the process works only in one direction, with the result that decryption is no longer possible using the public key. For that reason, anybody who wishes to receive an encrypted message may send a communication partner via an unsecured route the public key required to encrypt the message. The received message is then decrypted using a different key, the private key, which is kept secret and which is not forwarded to communication partners.¹⁸⁴ The process can best be understood on the basis of a comparison with a padlock: anyone can snap a padlock together and, by so doing, secure a trunk; the padlock can only be opened, however, by a person with the right key.¹⁸⁵ Although the public and private keys are linked, the private key cannot be calculated on the basis of the public key.

Ron Rivest, Adi Shamir and Leonard Adleman invented an asymmetric encryption process, which has been named after them (RSA process). In a one-way (trapdoor) function the result of the multiplication of two very large prime numbers

is used as a component of the public key. The text is then encrypted using that key. Decryption is dependent on knowledge of the two prime numbers employed. However, there is no known mathematical process by means of which the large integers resulting from the multiplication of two prime numbers can be factored in such a way as to determine what those prime numbers were. At present, all possible combinations must be tried systematically. Given the present state of mathematical knowledge, therefore, the process is secure, provided that sufficiently large prime numbers are chosen. The only risk is that at some stage a brilliant mathematician will discover a quicker factoring method. Thus far, however, even the best efforts have proved fruitless.¹⁸⁶ Many people even claim that the problem is insoluble, but this theory has not yet been proved.¹⁸⁷ By comparison with symmetric processes (e.g. DES), however, public-key encryption requires much more PC calculation time or the use of rapid, large-scale computers.

In order to make the public-key process generally accessible, Phil Zimmermann came up with the idea of linking the public-key process, which involves a great deal of calculation, with a faster symmetric process. The message itself should be encrypted using an asymmetric process, the IDEA [International Institute for Democracy and Electoral Assistance] process developed in Zurich, but the key to the symmetric encryption would be exchanged at the same time, as in the public-key process. Zimmermann developed a user-friendly program (Pretty Good Privacy), which created the requisite key and carried out the encryption at the push of a button (or the click of a mouse). The program was placed on the Internet, from where anyone could download it. PGP was ultimately bought by the US firm NAI, but is still made available to private individuals free of charge.¹⁸⁸

The source text for the earlier versions has been published, so it can be assumed that no backdoors have been incorporated. Unfortunately, the source texts for the newest version, PGP 7, which is characterized by an exceptionally user-friendly graphic interface, are no longer published. There

is, however, a further implementation of the Open PGP Standard: GnuPG. GnuPG offers the same encryption methods as PGP, and is also compatible with PGP. However, it is freeware, its source code is known and any individual can use it and pass it on. The Federal German Ministry for Economic Affairs and Technology has promoted the porting of GnuPG on Windows and the development of a graphic interface; unfortunately, however, these functions have not yet been fully developed. There are also rival standards to OpenPGP, such as S/MIME, which are supported by many e-mail programs.

In the future quantum cryptography may open up new prospects for secure key exchange. It would ensure that the interception of a key exchange could not pass unnoticed. If polarized photons are transmitted, the fact of their polarization cannot be established without altering that polarization. Eavesdroppers on the line could thus be detected with 100% certainty. Only those keys, which had not been intercepted, would then be used. In experiments, transmission over 48 km via fiber optic cable and over 500 m through the air has already been achieved.¹⁸⁹

In the discussion on the actual level of security of encryption processes the accusation has repeatedly been made that American products contain backdoors. For example, Excel made headlines here in Europe when it was suggested that in the European version of its program half the key is revealed in the file header. Microsoft also gained media attention when a hacker claimed to have discovered a NSA key hidden in the program, a claim that was of course strongly denied by Microsoft. Since Microsoft has not revealed its source code, any assessment amounts to pure speculation. At all events, the earlier versions of PGP and GnuPG can be said with a great degree of certainty not to contain such a backdoor, since their source text has been disclosed.

Many states initially ban the use of encryption software or cryptographic equipment and make exceptions only subject to prior authorization. The states concerned are not just dictatorships such as

China, Iran or Iraq. Democratic states have also imposed legal restrictions on the use or purchase of encryption programs or equipment. It would appear that communications are to be protected against being read by unauthorized private individuals, but that the state should retain the possibility of intercepting such communications, if necessary on the basis of specific legal provisions. The authorities' loss of technical superiority is thus made good by means of legal bans. For example, until recently France imposed a general ban on the use of cryptography, granting authorizations only in individual cases. A few years ago in Germany a debate arose concerning restrictions on encryption and the compulsory submission of a key to the authorities. In the past, the USA has taken a different course, imposing restrictions on key length.

By now, these attempts should have been shown, once and for all, to be futile. The state's interest in having access to encryption processes and thus to the plain texts does not only stand in opposition to the right to privacy, but also to entrenched economic interests. E-commerce and electronic banking are dependent on secure communications via the Internet. If this cannot be guaranteed, these techniques are doomed to failure, owing to a lack of customer confidence. This link explains the about-turn in US and French policy on cryptography.

It should be pointed out here that there are two reasons why e-commerce needs secure encryption processes: not only in order to encrypt messages, but also to prove beyond doubt the identity of business partners. The electronic signature procedure can be carried out using a reversal of the public-key process: the private key is used to encrypt the signature, and the public key to decrypt it. This form of encryption confirms the authenticity of the signature. Through the use of the public key, any individual can convince another of his or her genuineness, but he or she cannot imitate the signature itself. This function is also built into PGP as an additional user-friendly feature.

In some states business travelers are prohibited from using encryption programs on the laptop

computers they carry with them, ruling out any protection of communications with their own firm or the data stored on those computers.

When answering the question of what persons, and under what circumstances, should be advised to employ encryption, a distinction must be drawn between private individuals and firms. As far as private individuals are concerned, it must be clearly stated that the encryption of fax and telephone messages using a crypto-telephone or cipher-fax is not really a workable option, not only because the cost of purchasing such equipment is relatively high, but also because their use presupposes that the interlocutor also has such equipment available, which is doubtless only very rarely the case.

In contrast, e-mails can and should be encrypted by everyone. The oft-repeated claim that a person has no secrets and thus has no need to encrypt messages must be countered by pointing out that written messages are not normally sent on postcards. However, an unencrypted e-mail is nothing other than a letter without an envelope. The encryption of e-mails is secure and relatively straightforward and user-friendly systems, such as PGP/GnuPG, are already available, even free of charge, to private individuals on the Internet. Unfortunately, they are not yet sufficiently widely distributed. The public authorities should set a good example and employ encryption as a standard practice in order to demystify the process.

As far as firms are concerned, they should take strict measures to ensure that sensitive information is only transmitted via secure media. This may seem obvious, and no doubt is for large undertakings, but in small- and medium-sized firms in particular internal information is often transmitted via unencrypted e-mails, because awareness of the problem is not sufficiently well developed. In this connection, it can only be hoped that industry associations and chambers of commerce will step up their efforts to increase that awareness. Admittedly, the encryption of e-mails is only one security aspect amongst many, and serves no purpose if the information is made available to others prior to encryption.

The implication is that the entire working environment must be protected, thereby guaranteeing the security of a firm's premises, and checks must be carried out on persons entering offices and accessing computers. In addition, unauthorized access to information via the firm's network must be prevented by means of the introduction of corresponding firewalls. Here, particular dangers are posed by the linking of the firm's internal network and the Internet. If security is to be taken seriously, only those operating systems should be used whose source code has been published and checked, since only then can it be determined with certainty what happens to the data.

Firms are thus faced with a wide variety of tasks in the security sphere. Many businesses have already been set up to provide security advice and arrangements at affordable prices, and the supply of such services is expanding steadily in line with demand. In addition, however, it must be hoped that industry associations and chambers of commerce take up this issue, particularly in order to draw the attention of small firms to the problem of security and to support efforts to devise and implement comprehensive protection arrangements.

The EU's External Relations and Intelligence Gathering

With the adoption of the Maastricht Treaty in 1991, the Common Foreign and Security Policy (CFSP) was established in its most elementary form as a new policy instrument for the European Union. Six years later the Amsterdam Treaty gave further structure to the CFSP and created the possibility for common defense initiatives within the European Union, whilst maintaining the existing alliances. On the basis of the Amsterdam Treaty and with the experiences in Kosovo in mind, the Helsinki European Council of December 1999 launched the European Security and Defense Initiative.

This initiative aims at the creation of a multinational force of between 50 000 and 60 000 troops by the second half of 2003. The existence of such a multinational force will make

the development of an autonomous intelligence capacity inevitable. The simple integration of the existing WEU [Western European Union] intelligence capacity will be insufficient for this purpose. Further cooperation between the intelligence agencies of the Member States, well beyond the existing forms of cooperation, cannot be avoided.

However, the further development of the CFSP is not the only factor leading to closer cooperation among the Union's intelligence services. Further economic integration within the European Union will likewise necessitate a more intensive cooperation in the field of intelligence collection. A united European economic policy implies a united perception of economic reality in the world outside the European Union. A united position in trade negotiations within the WTO [World Trade Organization] or with third countries calls for joint protection of the negotiating position. Strong European industries need joint protection against economic espionage from outside the European Union.

It must finally be emphasized that further development of the Union's second pillar and the Union's activities in the field of Justice and Home Affairs will inevitably also lead to further cooperation between intelligence services. In particular, the joint fight against terrorism, illegal trade in arms, trafficking of human beings, and money laundering cannot take place without intensive cooperation between intelligence services.

Although there is a long tradition within the intelligence services of only trusting the information they collect themselves and maybe even of distrust between the different intelligence services within the European Union, cooperation between services is already gradually increasing.¹⁹⁰ Frequent contacts do exist within the framework of NATO, the WEU and within the European Union. And whereas, within the framework of NATO, the intelligence services are still heavily dependent on the far more sophisticated contributions from the United States, the establishment of the WEU satellite center in Torrejon (Spain) and the creation

of an intelligence section attached to the WEU headquarters have contributed to more autonomous European action in this field.

In addition to these developments already taking place, it must be emphasized that there are objective advantages to a joint European intelligence policy. First of all there is simply too much classified and unclassified material available to be collected, analyzed, and evaluated by any single agency or under any single bilateral agreement in Western Europe. The demands on intelligence services range from defense intelligence, through intelligence on third states' internal and international economic policies, to intelligence in support of the fight against organized crime and drug trafficking. Even if cooperation existed only on the most basic level, i.e. as regards the collection of open-source intelligence (OSINT), the results of this cooperation would already be of great importance for the European Union's policies.

In the recent past budgets for intelligence collection have been cut and, in some cases, are still being reduced. At the same time, the demand for information and therefore intelligence has grown. These reduced budgets do not only make this cooperation desirable but, in the long run, also profitable. In particular, in the case of establishing and maintaining technical facilities, joint operations are of interest when money is scarce but also when it comes to evaluating the collected information. Further cooperation will increase the effectiveness of intelligence collection.

In principle, collected intelligence is used to give governments the possibility of better and better-founded decision-making. Further political and economic integration in the European Union demands that intelligence should be available at European level and should also be based on more than one single source.

These objective advantages merely illustrate the growing importance of cooperation within the European Union. In the past nation states used to guarantee their own external security, internal

order, national prosperity and cultural identity. Today, the European Union is in many fields in the process of taking up a role at least complementary to that of the nation state. It is inconceivable that the intelligence services will be the last and only area not affected by the process of European integration.

Following the Second World War cooperation in the field of intelligence collection did not at first take place at European level, but far more at transatlantic level. It has already been shown that very close relations in the field of intelligence gathering were established between the United Kingdom and the United States. But also in the field of defense intelligence within the framework of NATO and beyond, the United States was and still is the absolutely dominant partner. The major question therefore is this: will growing European cooperation in the field of intelligence gathering seriously disrupt relations with the United States, or might it lead to a strengthening of those relations? How will EU/US relations develop under the new Bush Administration? And, in particular, how will the special relationship between the United States and the United Kingdom be maintained in this framework?

Some take the view that there need not be a contradiction between the British/US special relationship and the further development of the CFSP. Others believe that intelligence gathering may be precisely the issue which forces the United Kingdom to decide whether its destiny is European or transatlantic. Britain's intimate links with the US (and with the other partners in the UKUSA Agreement) may make it more difficult for other EU states to share intelligence amongst themselves—because the United Kingdom may be less interested in intra-European sharing, and because its EU partners may trust the United Kingdom less.

Equally, if the US believes that the United Kingdom has developed special links with its EU partners, and that this is part of a European special agreement, the US may become reluctant to continue sharing its intelligence with the United

Kingdom. Closer EU cooperation in the field of intelligence may therefore constitute a serious test of the European ambitions of the United Kingdom and of the EU's capacity for integration.

In the present circumstances it is, however, highly unlikely that even extremely rapid progress in cooperation among the European partners can, in the short and even in the longer term, offset the technological advantage enjoyed by the United States. The European Union will not be able to establish a sophisticated network of SIGINT satellites, imaging satellites and ground stations. The European Union will not be able to develop, in the short term, the highly sophisticated network of computers required for the selection and evaluation of the collected material. The European Union will not be prepared to make available the budgetary resources needed to develop a true alternative to the intelligence efforts of the United States.

Purely from a technological and budgetary viewpoint, therefore, it will be in the interests of the European Union to maintain a close relationship with the United States in the field of intelligence collection. But also from a more political point of view, it will be important to maintain and, where necessary, strengthen relationships with the United States, in particular in the context of the joint fight against organized crime, terrorism, drugs and arms trafficking and money laundering. Joint intelligence operations are necessary to support a joint fight. Joint peacekeeping actions, such as in former Yugoslavia, demand a greater European contribution in all areas.

On the other hand, growing European awareness should be accompanied by greater European responsibility. The European Union should become a more equal partner, not only in the economic field, but also in the field of defense and therefore in the field of intelligence collection. A more autonomous European intelligence capacity should therefore not be seen as weakening transatlantic relations, but should be used to strengthen them by establishing the European Union as a more equal and more capable partner. At the same time, the European Union must make independent efforts to

protect its economy and its industry against illegal and unwanted threats such as economic espionage, cyber-crime, and terrorist attacks.

However, transatlantic understanding is necessary in the field of industrial espionage. The European Union and the United States should agree on a set of rules laying down what is and what is not allowed in this area. With a view to strengthening transatlantic cooperation in this field, a joint initiative could be undertaken at WTO level using that organization's mechanisms to safeguard fair economic development worldwide.

Although the issue of the protection of European citizens' privacy must remain fundamental, the further development of a joint European Union intelligence capacity should be considered necessary and inevitable. Cooperation with third countries, and in particular the United States, should be maintained and, very possibly, strengthened. This does not necessarily mean that European SIGINT activities should automatically be integrated in an independent European Union ECHELON system, or that the European Union should become a full partner in the present UKUSA Agreement. However, the development of proper European responsibility in the field of intelligence collection must be actively considered. An integrated European intelligence capacity demands, at the same time, a system of European political control over the activities of these agencies. Decisions will have to be taken on the procedure for assessing intelligence and for taking the political decisions, which result from an analysis of intelligence reports. The lack of such a system of political control, and therefore of political awareness and responsibility for the process of intelligence collection, would be detrimental to the process of European integration.

Conclusions and Recommendations

That a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no

longer in doubt. It may be assumed, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organizations, including American sources, that the system or parts of it were, at least for some time, code-named ECHELON. What is important is that its purpose is to intercept private and commercial communications, and not military communications.

Analysis has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed. Nevertheless, it is worrying that many senior Community figures, in particular European Commissioners, who gave evidence to the Temporary Committee claimed to be unaware of this phenomenon.

The surveillance system depends, in particular, upon worldwide interception of satellite communications. However, in areas characterized by a high volume of traffic only a very small proportion of those communications is transmitted by satellite. This means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals. However, inquiries have shown that the UKUSA states have access to only a very limited proportion of cable and radio communications, and, owing to the large numbers of personnel required, can analyze only an even smaller proportion of those communications. However extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice.

Since intercepting communications is a method of spying commonly employed by intelligence services, other states might also operate similar systems, provided that they have the required funds and the right locations. France, thanks to its overseas territories, is the only EU Member State, which is geographically and technically capable of operating a global interception system by itself. There is ample evidence that Russia also operates such a system.

As regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios. If a system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union, although at present that title lays down no provisions on the subject, so no criteria are available. If, on the other hand, the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition. If a Member State participates in such a system, it violates EC law. At its meeting of 30 March 2000 the Council made clear that it cannot agree to the creation or existence of an interception system which does not comply with the rules laid down in the laws of the Member States and which breaches the fundamental principles designed to safeguard human dignity.

Any interception of communications represents serious interference with an individual's exercise of the right to privacy. Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference. Interference must be proportionate: thus competing interests need to be weighed up and it is not enough that the interference should merely be useful or desirable.

An intelligence system, which intercepted communications permanently and at random, would be in violation of the principle of proportionality and would therefore not be compatible with the ECHR. It would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable.

Since most of the rules governing the activities of US intelligence services abroad are classified, compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and predictability laid down by the European Court of Human Rights probably occur.

Although the USA is not itself an ECHR contracting party, the Member States must nevertheless act in a manner consistent with the ECHR. The Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and predictability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

In addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus. As the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinizing the secret services.

As the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and since in some cases parliamentary monitoring bodies do not even exist, the degree of protection can hardly be said to be adequate. It is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinizing the activities of the intelligence services. But even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it

is only the former which affect their own citizens. In the event of cooperation between intelligence services under the CFSP and between the security authorities in the spheres of justice and home affairs, the institutions must introduce adequate measures to protect European citizens.

Part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc. For these reasons, the firms concerned are often subject to surveillance. The US intelligence services do not merely gather general economic intelligence, but also intercept communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery.

Detailed interception poses the risk that information may be used as competitive intelligence, rather than combating corruption, even though the US and the United Kingdom state that they do not do so. However, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled. It should also be pointed out that an agreement on combating the bribery of officials, under which bribery is a crime at the international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications. At all events, it must be made clear that the situation becomes intolerable when intelligence services allow themselves to be used for purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country. Although it is frequently maintained that the global interception system considered in this report has been used in this way, no such case has been substantiated.

The fact is that sensitive commercial data are mostly kept inside individual firms, so that

competitive intelligence-gathering primarily involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else, more and more frequently, by hacking into internal computer networks. Only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence gathering. This applies systematically in the following three cases:

- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;
- in the case of videoconferencing within multinationals using VSAT or cable;
- if vital contracts are being negotiated on the spot (e.g. for the building of plants, the development of telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the company's head office.

Risk and security awareness in small and medium-sized firms is unfortunately often inadequate and the dangers of economic espionage and the interception of communications are often not recognized. Since security awareness is likewise not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations), immediate action is therefore necessary.

Firms must secure the whole working environment and protect all communications channels which, are used to send sensitive information. Sufficiently secure encryption systems exist at affordable prices on the European market. Private individuals should also be urged to encrypt e-mails: an unencrypted e-mail message is like a letter without an envelope. Relatively user-friendly systems exist on the Internet which are even made available for private use free of charge.

In December 1999 in Helsinki the European Council decided to develop more effective

European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP. In order to achieve this goal, by the year 2003 the Union was to be able to rapidly deploy units of about 50000—60000 troops which should be self-sustaining, including the necessary command, strategic reconnaissance and intelligence capabilities. The first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee.

Cooperation among intelligence services within the EU seems essential on the grounds that, firstly, a common security policy, which did not involve the secret services, would not make sense and, secondly, it would have numerous professional, financial and political advantages. It would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR. The European Parliament would of course have to exercise appropriate monitoring. The European Parliament is in the process of implementing the Regulation (EC) No 1049/2001 on public access to European Parliament, Council and Commission documents by revising the provisions of its Rules of Procedure as regards access to sensitive documents.

Recommendations

Conclusion and amendment of international agreements on the protection of citizens and firms.

1. The Secretary-General of the Council of Europe is called upon to submit to the Ministerial Committee a proposal to protect private life, as guaranteed in Article 8 of the ECHR, brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the

European Court of Human Rights nor reduce the flexibility, which is vital if future developments are to be taken into account.

2. The Member States of the European Union are called upon to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens rights in order to scrutinize the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of this report, and in particular Section 8.3.4., as derived from Article 8 of the ECHR.
3. The member countries of the Council of Europe are called upon to adopt an additional protocol, which enables the European Communities to accede to the ECHR or to consider other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities.
4. The Member States are called upon, at the next Intergovernmental Conference, to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy. The EU institutions are called upon to comply with the fundamental rights laid down in the Charter in their respective areas of responsibility and activity.
5. The European Union and the USA are called upon to conclude an agreement on the basis of which each party applies to the other the rules governing the protection of privacy and the confidentiality of business communications which are valid for its own citizens and firms.
6. The Member States are called upon to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions.
7. The UN Secretary-General is called upon to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations.
8. The USA is called upon to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the Covenant by the USA can be submitted to the Human Rights Committee set up under the Covenant. The relevant US NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), are called upon to exert pressure on the US Administration to that end.
9. The Council and the Member States are strongly urged to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level. The European Parliament should play an important role in this monitoring and control system.
10. The Member States are strongly urged to review their own legislation on the operations of the intelligence services to ensure that it is consistent with the fundamental rights laid

-
- down in the ECHR and in the case law of the European Court of Human Rights and, if necessary, to adopt appropriate legal provisions. They are called upon to afford all European citizens the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence. Any of their laws, which are discriminatory in terms of the surveillance powers granted to the secret services, must be repealed.
11. The Member States are called upon to aspire to a common level of protection against intelligence operations and, to that end, to draw up a code of conduct based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services. A similar code of conduct should be negotiated with the USA.
 12. The Member States are called upon to pool their communications interception resources with a view to enhancing the effectiveness of the CFSP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission.
 13. The Member States are called upon to consider to what extent industrial espionage and the payment of bribes as a way of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void. The USA, Canada, Australia and New Zealand are called upon to join this initiative.
 14. The Member States are called upon to give a binding undertaking neither to engage in industrial espionage, either directly or behind the front offered by a foreign power active on their territory, nor to allow a foreign power to carry out such espionage from their territory, thereby acting in accordance with the letter and spirit of the EC Treaty.
 15. The Member States and the US Administration are called upon to start an open US-EU dialogue on economic intelligence gathering.
 16. The authorities of the United Kingdom are called upon to explain their role in the UK/USA alliance in connection with the existence of a system of the ECHELON type and its use for the purposes of industrial espionage.
 17. The Member States are called upon to ensure that their intelligence services are not misused for the purposes of obtaining competitive intelligence, since this would be at odds with the Member States' duty of loyalty and the concept of a common market based on free competition.
 18. The Member States are called upon to guarantee appropriate parliamentary and legal monitoring of their secret services. Those national parliaments, which have no monitoring body responsible for scrutinizing the activities of the intelligence services, are called upon to set up such a body.
 19. The monitoring bodies responsible for scrutinizing the activities of the secret services are called upon, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals.

-
20. The Member States' intelligence services are called upon to accept data from other intelligence services only in cases where such data has been obtained in accordance with the conditions laid down by their own domestic law, as Member States cannot evade the obligations arising from the ECHR by using other intelligence services.
21. Germany and the United Kingdom are called upon to make the authorization of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorized or even merely tolerated on their territory respect human rights.
22. The Commission and Member States are called upon to inform their citizens and firms about the possibility of their international communications being intercepted. This information must be combined with practical assistance in developing and implementing comprehensive protection measures, not least as regards IT security.
23. The Commission, the Council and the Member States are called upon to develop and implement an effective and active policy for security in the information society. As part of that policy, specific attention should be given to increasing the awareness of all users of modern communication systems of the need to protect confidential information. A Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies must be established.
24. The Commission and Member States are urged to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software.
25. The Commission and Member States are called upon to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programs. The Commission is called upon to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the ,least reliable category.
26. The European institutions and the public administrations of the Member States are called upon systematically to encrypt e-mails, so that ultimately encryption becomes the norm.
27. The Community institutions and the public administrations of the Member States are called upon to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses.
28. The Commission is instructed to have a security analysis carried out, which will show what needs to be protected, and to have a protection strategy drawn up.
29. The Commission is called upon to update its encryption system in line with the latest developments, given that modernization is urgently needed, and calls on the budgetary authority (the Council together with Parliament) to provide the necessary funding.
30. The competent committee is requested to draw up an own-initiative report on security and the protection of secrecy in the European institutions.
31. The Commission is called upon to ensure that data is protected in its own IT systems and to

step up the protection of secrecy in relation to documents not accessible to the public.

32. The Commission and the Member States are called upon to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Program.
33. Firms are called upon to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency.
34. The Commission is called upon to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centers—in particular in those Member States where such centers do not yet exist—to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance.
35. The Commission is called upon to pay particular attention to the position of the applicant countries; if their lack of technological independence prevents them from implementing the requisite protective measures they should be given support.
36. The European Parliament is called upon to hold an international congress on the protection of privacy against telecommunications surveillance in order to provide NGOs from Europe, the USA and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action.

***Minority Opinion by Giuseppe Di Lello,
Pernille Frahm and Alain Krivine***

The report by the Temporary Committee confirms the existence of the Echelon interception system, which is administered by various countries, including the United Kingdom, a Member

State of the European Union, with the cooperation of Germany. An interception system of this nature, which does not differentiate between communications, data and documents, infringes the fundamental right to privacy guaranteed by Article 8 of the European Convention on Human Rights and Article 6 of the Treaty on European Union.

The system therefore flagrantly infringes the freedoms enjoyed by European citizens, the logic of the free market and the security of the Union. Whatever our support for or opposition to that logic and those treaties may be, such infringements are unacceptable. In its conclusions, the report ought to have called on the United Kingdom to dissociate itself from the Echelon system and on Germany to close the listening post located on its soil. It is a matter of regret that the European Union is more preoccupied with industrial espionage than with individual monitoring.

***Minority Opinion by Patricia McKenna and
Ilka Schröder***

This report makes an important point in emphasizing that Echelon does exist, but it stops short of drawing political conclusions. It is hypocritical for the European Parliament to criticize the Echelon interception practice while taking part in plans to establish a European Secret Service.

No effective public control mechanism of secret services and their undemocratic practices exists globally. It is in the nature of secret services that they cannot be controlled. They must therefore be abolished. This report serves to legitimize a European Secret Service, which will infringe fundamental rights—just as Echelon does.

For the majority in Parliament, the focus is industry, where profit interests are supposedly threatened by industrial espionage. However, the vital issue is that no one can communicate in confidence over distances any more. Political espionage is a much greater threat than economic espionage.

This report constantly plays down these dangers of Echelon, while it remains silent about plans to introduce the ENFOPOL interception system in the EU. Every society must take a fundamental decision whether or not to live under permanent control. By adopting this report, the European Parliament shows that it is not concerned about protecting human rights and citizens' liberties.

Minority Opinion by Jean-Charles Marchiani

The UEN [Union for Europe of the Nations] Group was not surprised at the outcome of the vote on Mr. Schmid's report which, originally, was supposed to concern itself with the Echelon espionage system set up by certain English-speaking countries. From the outset, a majority within Parliament had clearly indicated its intentions, preferring to set up this temporary committee rather than a full-blown committee of inquiry. Accordingly, it had nothing else to fear from proceedings where the reporter's ability to create regular diversions was in no way threatened by a band of malcontents whose motives were too disparate.

Our message is crystal-clear: Mr. Schmid's efforts have been unable to conceal either the existence of the Echelon system or the active or passive involvement of several Member States. That has resulted in a serious breach of the principles underlying the treaties which ought to have led to sanctions being imposed or, at the very least, to measures being taken which might prevent intra-European solidarity from being subordinated to the imperatives of the solidarity of the English-speaking world. Mr. Schmid's weighty report is rich in information but does not properly address the central issue.

We therefore wish to distance ourselves from it and to reject a procedure, which enables this Parliament, on the one hand, to take preventive sanctions against a democratically elected government and, on the other, to refrain from so doing in instances such as this one.

Minority Opinion by Maurizio Turco

- A. Although the likely existence of an Anglo-American system for the systematic and generalized interception of communications using search engines has been demonstrated, no reference is made to the fact that this technological capacity is certainly being used by Germany and the Netherlands and, probably, by France as well. Accordingly, since the secret services are intercepting communications from abroad, without authorization and on the grounds of national security, some Member States will be intercepting communications from institutions, citizens or businesses of other Member States.
- B. Although more powerful encryption methods should help to protect privacy, their introduction will inevitably lead to the appearance of more powerful lawful means of decryption techniques, given the indissoluble link between the development of cryptographic, code-breaking and technical interception systems.
- C. Solutions must therefore be sought in the political field:
- via legal and parliamentary scrutiny of interception activities and monitoring of the police, security and intelligence services;
 - by preventing the proliferation of control bodies which operate to different data-protection standards and without any genuine democratic and legal scrutiny,
 - by regulating CE on the basis of the highest standard and the case-law of the ECHR—protection of the privacy of European citizens against preventive interference by government authorities and eliminating the discrimination existing within the European Union between citizens of various Member States.

Endnotes

¹ Voice of America, 23 February 2000.

² Voice of America, 30 March 2000.

³ STOA (Scientific and Technological Options Assessment) is a department of the Directorate General for Research of the European Parliament, which commissions research at the request of committees. However, the documents it produces are not subject to scientific review.

⁴ Duncan Campbell, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in STOA (Ed.), Development of Surveillance Technology and Risk of Abuse of Economic Information (October 1999), PE 168.184.

⁵ Steve Wright, An appraisal of technologies of political control, STOA interim study, PE 166.499/INT.ST. (1998).

⁶ Duncan Campbell, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in STOA (Ed.), Development of Surveillance Technology and Risk of Abuse of Economic Information (October 1999), PE 168.184., PE 305.391 22/194 RR\445698EN.doc.

⁷ Raytheon Corp Press release, <http://www.raytheon.com/sivam/contract.html>; Scott Shane, Tom Bowman, "America's Fortress of Spies," *Baltimore Sun*, 3 December 1995.

⁸ European Parliament decision of 5 July 2000, B5-0593/2000, OJ C 121/131 of 24 April 2001.

⁹ Decision of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry (95/167/EC), Article 3(3)-(5)..RR\445698EN.doc 23/194 PE 305.391.

¹⁰ The Commission on the Roles and Capabilities of the US Intelligence Community has stated in its report, *Preparing for the 21st Century: An Appraisal of US Intelligence* (1996) that 95% of all economic intelligence is derived from open sources (Chapter 2, "The Role of Intelligence").

¹¹ Foreign communications is all incoming and outgoing civilian, military or diplomatic communications. If the intelligence service has access to the relevant cables, it can intercept both incoming and outgoing

communications. If the service targets satellite communications, it has access only to the downlink, but can intercept all the communications it carries, including those not intended for its own territory. Since as a rule the satellite footprints cover the whole of Europe or an even wider area, satellite communications throughout Europe can be intercepted using receiving stations in one European country. The + indicates that communications are intercepted. The – signifies that communications are not intercepted.

¹² With the aid of a demonstration version of Visual Route, a program, which reveals the route taken by an Internet link, it was shown that a link from Germany to England, Finland, or Greece passes via the USA and the UK. A link from Germany to France likewise passes via the UK. Links from Luxembourg to Belgium, Greece, Sweden, or Portugal pass via the USA and to Germany, Finland, France, Italy, the Netherlands or Austria via the switch in London. <http://visualroute.cgan.com.hk/>.

¹³ Letter from the Minister of State in the German Federal Defense Ministry, Walter Kolbow, to the reporter, dated 14 February 2001.

¹⁴ Süddeutsche Zeitung No 80, 5.4.2001, 6.

¹⁵ Jeffrey T. Richelson, *The U.S. Intelligence Community* (1989), 188, 190.

¹⁶ Letter from the Minister of State in the German Federal Defense Ministry, Walter Kolbow, to the reporter, dated 14 February 2001.

¹⁷ Major A. Andronov, *Zarubezhnoye voyennoye obozreniye*, No 12, 1993, 37-43.

¹⁸ Until May 2001 the FIS was not authorized to intercept foreign cable communications in Germany.

¹⁹ Law on the restriction of the privacy of posts and telecommunications (law on Article 10 of the Basic Law) of 13 August 1968.

²⁰ Information drawn from the answers given to the Temporary Committee by telecommunications service providers from a number of Member States.

²¹ Deutsche Telekom homepage: www.detesat.com/deutsch/

²² Georg E. Thaller, *Satellites in Earth Orbit*, Franzisverlag (1999).

²³ Cf. Hans Dodel, *Satellite communications*, Huthig Verlag (1999).

²⁴ Homepage of the Federation of American Scientists, <http://www.geo-orbit.org>.

²⁵ Nicky Hager, *Exposing the Global Surveillance System* <http://www.ncoic.com/echelon1.htm>; *Secret Power. New Zealand's Role in the International Spy Network*, Craig Potton Publishing, 1996.

²⁶ Jeffrey T. Richelson, *Desperately Seeking Signals*, *The Bulletin of American Scientists*, Vol. 56, No. 2,

47-51; <http://www.bullatomeci.org/issues/2000/ma00/ma00richelson.html>. See also Richelson, T. Jeffrey, *The U.S. Intelligence Community*, Westview Press, 1999.

²⁷ Duncan Campbell, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition, Part 4/5, in STOA (Ed.). *Development of Surveillance Technology and Risk of Abuse of Economic Information*, October 1999, <http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf>. Inside Echelon, 25.7.2000, <http://www.heise.de/tp/deutsch/special/ech/6928/1.html>. Interception Capabilities Impact and exploitation: Echelon and its role in COMINT, submitted to the Temporary Committee on 22 January 2001.

²⁸ Jeffrey T. Richelson, Newly released documents on the restrictions NSA places on reporting the identities of US persons, Declassified. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html>.

²⁹ Military.com; *.mil-Homepages.

³⁰ Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet, *Securing our Nation's Safety* (2000), <http://www.dpmc.govt.nz/dess/securingoursafety/index.html>.

³¹ Abbreviations used: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Squadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

³² It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded field stations', from the home page of the 544th Intelligence Group <http://www.aia.af.mil>.

³³ Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; <http://www.aph.gov.au/hansard> 52 Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; <http://www.aph.gov.au/hansard>.

³⁴ Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet "Securing our Nation's Safety," December 2000, <http://www.dpmc.govt.nz/dess/securingoursafety/index.html>

³⁵ Ibid. In 1989, [...] the GCSB opened its satellite communications interception station at Waihopai, near Blenheim. [...] The signals intelligence is obtained from a variety of foreign communications and other non-communications signals, such as radar. The GCSB not only intercepts the signals, it also processes, decrypts

or decodes and/or translates the information the signals contain before passing it on as a report to the appropriate Minister or government department.

³⁶ Nicky Hager, *Secret Power*. New Zealand's Role in the International Spy Network, op cit., p. 182.

³⁷ Announcement of 31 May 2001 on the INSCOM homepage, http://www.vulcan.belvoir.army.mil/bas_to_close.asp.

³⁸ Christopher Andrew, The making of the Anglo-American SIGINT Alliance in Hayden B. Peake, Samuel Halpern (Eds.), *In the Name of Intelligence*. Essays in Honor of Walter Pforzheimer, NIBC Press (1994), 95 -109.

³⁹ Christopher Andrew, The making of the Anglo-American SIGINT Alliance, op cit., p. 99 At a meeting in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that "it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable," and said that "the time had come or a free exchange of intelligence." (quoted from COS (40)289, CAB 79/6, PRO. Smith, *The Ultra Magic Deals*, 38, 43-4. Sir F.H. Hinsley, et al., *British Intelligence in the Second World War*, Vol. I, 312-13).

⁴⁰ Christopher Andrew, The making of the Anglo-American SIGINT Alliance, op cit., p.100. In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liaison officer to the British Joint Services Mission in Washington, Tim O'Connor, to advise him on cryptologic collaboration.

⁴¹ Ibid, p.100. Sir F.H. Hinsley, et al., *British Intelligence in the Second World War*, Vol. II, 56.

⁴² Christopher Andrew, op. Cit. P. 101. Sir F.H. Hinsley, et al., op. Cit. p. 48.

⁴³ Christopher Andrew, op. cit., p. 101-2. Interviews with Sir F.H. Hinsley, "Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 June 1945, Tab A, RG 457 SRH-110, NAW 63 Harry S. Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: "The Secretary of War and the Secretary of the Navy are hereby authorized to direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Operations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States."

⁴⁴ Bradley F. Smith, *The Ultra-Magic Deals and the Most Secret Special Relationship*, Novato, Ca: Presidio,

1993.

⁴⁵ Christopher Andrew, *The making of the Anglo-American SIGINT Alliance* in Hayden, H. Peake and Samuel Halpern Eds, *In the Name of Intelligence. Essays in Honor of Walter Pforzheimer* (NIBC Press 1995) p. 95. Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing.

⁴⁶ Intelligence and Security Committee Annual Report 1999-2000. Presented to Parliament by the Prime Minister by Command of Her Majesty, November 2000, 8, 14.

⁴⁷ Domestic and External Secretariat of the Department of the Prime Minister and Cabinet of New Zealand, *Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies* (2000).

⁴⁸ Terms/Abbreviations/Acronyms' published by the US Navy and Marine Corps Intelligence Training Center (NMITC) at <http://www.cnet.navy.mil/nmitc/training/u.html>.

⁴⁹ Martin Brady, Head of the DSD, letter of 16.3.1999 to Ross Coulthart, Sunday Program Channel 9.

⁵⁰ Christopher Andrew, *The growth of the Australian Intelligence Community and the Anglo-American Connection*, pp. 223-4.

⁵¹ Jeffrey T. Richelson, *The National Security Agency Declassified*, National Security Archive Electronic Briefing Book No 24, George Washington University <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html>.

⁵² Jeffrey T. Richelson, *The National Security Agency Declassified*, National Security Archive Electronic Briefing Book No 24, George Washington University <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html>.

⁵³ Statement for the Record of NSA Director Lt. Gen. Michael V. Hayden, USAF before the House Permanent Select Committee on Intelligence, April 12, 2000.

⁵⁴ Farewell from Vice Admiral William O. Studeman to NSA Employees, April 8 1992.

⁵⁵ Document 7. United States Signals Intelligence Directive [USSID] 18, "Legal Compliance and Minimization Procedures," July 27 1993.

⁵⁶ Document 2a. Memorandum from President Harry S. Truman to the Secretary of State, the Secretary of Defense, Subject: Communications Intelligence Activities, October 24 1952. Document 2b. National Security Council Intelligence Directive No. 9, Communications Intelligence, December 29 1952.

⁵⁷ Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security

Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3 1991.

⁵⁸ Document 12. 'Activation of Echelon Units,' from History of the Air Intelligence Agency, 1 January – 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

⁵⁹ Duncan Campbell, *Inside ECHELON. The history, structure and function of the global surveillance system known as ECHELON*, 1 97 Homepage of the Advocacy Center, <http://www.ita.doc.gov/td/advocacy/index.html>.

⁶⁰ Bo Elkjaer, Kenan Seeberg, *ECHELON singles out the Red Cross, A bombshell in the surveillance scandal: The organization is a possible surveillance target*, Ekstra Bladet, Denmark, 8.3.2000, <http://cryptome.org/echelon>.

⁶¹ Bo Elkjaer, Kenan Seeberg, *ECHELON was my baby: Interview with Margaret Newsham*, Ekstra Bladet, 17.1.1999

⁶² NBC TV interview '60 Minutes', 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

⁶³ Communication Security Establishment, subordinate to the Canadian Ministry of Defense, engaged in SIGINT

⁶⁴ NBC TV interview '60 Minutes', 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

⁶⁵ Florian Rötzer, *Die NSA geht wegen ECHELON an die Öffentlichkeit*; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special.

⁶⁶ NBC TV interview '60 Minutes', 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

⁶⁷ Interview on the Australian Channel 9 on 23.3.1999; <http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm>.

⁶⁸ Jim Bronskill, *Canada a key snooper in huge spy network*, Ottawa Citizen, 24.10.2000, <http://www.ottawacitizen.com/national/990522/2630510.html>.

⁶⁹ James Woolsey, Remarks at the Foreign Press Center, Transcript, 7.3.2000, <http://cryptome.org/echelon-cia.htm>.

⁷⁰ Commons Written Answers, House of Commons Hansard Debates

⁷¹ Ibid. 12.7.1995.

⁷² Ibid. 25.10.1994.

⁷³ Ibid. 3.12.1997

⁷⁴ Ibid. 12.5.2000.

⁷⁵ Ibid. 12.7.1995.

⁷⁶ Ibid. 8.3.1999, 6.7.1999.

⁷⁷ Ibid. 3.12.1997.

⁷⁸ Intelligence and Security Committee (UK), Annual Report 1999-2000, para. 14, presented to the Commons by the Prime Minister in November 2000.

⁷⁹ Defense Signals Directorate, Australian intelligence service engaged in SIGINT.

⁸⁰ Letter of 16.3.1999 from Martin Brady, Director of the DSD, to Ross Coulthart, 'Sunday' program; see also: http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

⁸¹ Domestic and External Secretariat of the Department of the Prime Minister and Cabinet of New Zealand, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000).

⁸² Brief aan de Tweede Kamer betreffende 'Het grootschalige af luisteren van moderne telecommunicatie systemen', 19.1.2001.

⁸³ Francesco Sorti, Dossier esclusivo. Caso ECHELON. Parla Luigi Ramponi. Anche i politici sapevano, Il mondo, 17.4.1998.

⁸⁴ Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'. Relazione del comitato parlamentare per I servizi di informazione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000. Trasmessa alle Presidenze il 19 dicembre 2000.

⁸⁵ Jean Guisnel, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998. Vincent Jauvert, Espionnage, comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, No 1900, 14 et seq.

⁸⁶ Erich Schmidt-Eenboom, in: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg (1999), 180.

⁸⁷ Russian Federation Federal Law on Foreign Intelligence, adopted by the Duma on 8 December 1995, Sections 5 and 11 141 Quoted in Gordon Bennett, Conflict Studies and Research Centre, The Federal Agency of Government communications and Information, August 2000, <http://www.csrc.ac.uk/pdfs/c105.pdf>.

⁸⁸ Art. 3(1) and Recital 15 "Where such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the Treaty on European Union, the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of the Treaty on European Union."

⁸⁹ See, for example, para 25 of the resolution on the draft action plan of the Council and Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice (13844/98 -C4- 0692/98 - 98/0923(CNS)), OJ C 219, 30.7.1999, p. 61 et seq.

⁹⁰ In the area of telecommunications surveillance there

are currently only two EU legislative acts, neither of which covers the question of admissibility: - Council resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 4.11.1996), the annex to which sets out the technical requirements relating to the lawful interception of modern telecommunications systems, and - Council Act of 29 May 2000 establishing, in accordance with Article 34 of the Treaty on European Union.

⁹¹ German Federal Constitutional Court (FCC), 1 BVR 226/94 of 14 July 1999, Rz 187: "The recording of data already represents a violation of that right in so far as it makes the content of the communications available to the Federal Intelligence Service and forms the basis of the ensuing analysis using search terms."

⁹² Compare the report submitted to the US Congress in late February 2000, "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance," <http://www.fas.org/irp/nsa/standards.html>, which refers to the Foreign Intelligence Surveillance Act (FISA), printed in Title 50, Chapter 36, USC, § 1801 et seq, and Executive Order No 12333, 3 CFR 200 (1982), printed in Title 50, Chapter 15, USC, § 401 et seq, <http://www4.law.cornell.edu/uscode750/index.html>.

⁹³ Article 12 of the Universal Declaration of Human Rights; Article 17 of the UN Covenant on Civil and Political Rights; Article 7 of the EU Charter of Fundamental Rights; Article 8 of the ECHR; Recommendation of the OECD Council on guidelines for the security of information systems, adopted on 26/27 November 1993, C(1992) 188/final; Article 7 of the Council of Europe Convention on the Protection of Persons with regard to the automatic processing of personal data; compare the study commissioned by STOA entitled "Development of Surveillance Technology and Risk of Abuse of Economic Information;" Part. 4/5: the legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), October 1999, 2.

⁹⁴ Adopted by the UN General Assembly on 16 December 1966.

⁹⁵ Optional Protocol to the International Covenant on Civil and Political Rights, adopted by the UN General Assembly on 16 December 1966.

⁹⁶ "Everyone has the right to respect for his or her private family life, home and communications."

⁹⁷ Judgment of the European Court of Human Rights, Loizidou/Turkey, 23.3.1995, line 62, with further references: '– the concept of 'jurisdiction' under this provision is not restricted to the national territory of the High Contracting Parties [–] responsibility can be

involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory', with reference to the European Court of Human Rights, Drozd and Janousek, 26.6.1992, line 91. See also the comprehensive details in Francis G. Jacobs, Robin C. A. White, *The European Convention on Human Rights*, Clarendon Press (1996), pp. 21 et seq. Jochen Abr. Frowein, Wolfgang Peukert, *European Convention on Human Rights*, N.P. Engel Verlag (1996), Rz 4 et seq.

⁹⁸ See European Court of Human Rights, Klass et al, 9.1978, line 41.

⁹⁹ See European Court of Human Rights, Malone, 2.8.1984, line 83 et seq; also B. Davy/U.Davy, *Aspects of state information collection and Article 8 of the ECHR*, JBI 1985, 656.

¹⁰⁰ Under the case law of the European Court of Human Rights (in particular Sunday Times, 26.4.1979, line 47 et.

¹⁰¹ Silver et al, 25.3. 1983, line 87 et seq. seq, Silver et al, 25.3.1983, line 85 et seq, the term 'the law' in Article 8(2) embraces not only laws in the formal sense, but also legal provisions below the level of a law and, in certain circumstances, even unwritten law. It is essential, however, that it is clear to the legal subject under what circumstances interference is possible. For more details see Wolfgang Wesseley, *Telecommunications Privacy; an unknown basic right?*, ÖJZ 1999, pp. 491 et seq, 495.

¹⁰² The justification of 'economic well-being' was accepted by the European Court of Human Rights in a case involving the transmission of medical data relevant to the award of public compensation, M.S./Sweden, 27.8.1997, line 38; and in a case involving the expulsion from the Netherlands of a person who had been living on welfare payments after the grounds for the award of a residence permit had ceased to apply, Ciliz/Netherlands, 11.7.2000, line 65.

¹⁰³ European Court of Human Rights, Leander, 26.3.1987, line 51.

¹⁰⁴ European Court of Human Rights, Malone, 2.8.1984, line 67.

¹⁰⁵ European Court of Human Rights, Leander, 26.3.1987, line 59, Sunday Times, 26.4.1979, line 46 et seq.

¹⁰⁶ European Court of Human Rights, Silver et al, 24.10.1983, line 97.

¹⁰⁷ European Court of Human Rights, Leander, 26.3.1987, line 60.

¹⁰⁸ Your reporter is aware that neither Luxembourg nor Ireland has a foreign intelligence service and does not carry out SIGINT operations. The need for a

specific supervisory body relates here only to domestic intelligence activities.

¹⁰⁹ For details of the situation regarding the supervision of intelligence services in the Member States, see Chapter 9.

¹¹⁰ Bill entitled 'Proposition de loi tendant à la création de délégations parlementaires pour le renseignement, and the related report by Arthur Paecht, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. novembre 1999.

¹¹¹ See also Dimitri Yernault, 'ECHELON and Europe. The protection of privacy against communications espionage', *Journal of the Courts, European Law*, 2000, 187 et seq.

¹¹² European Court of Human Rights, Abdulaziz, Cabales and Balkandali, 28.5.1985, line 67; X and Y/Netherlands, 26.3.1985, line 23; Gaskin v United Kingdom, 7.7.1989, line 38; Powell and Rayner, 21.2.1990, line 41.

¹¹³ This is also necessary for compliance with Article 13 of the ECHR, which grants the person whose privacy has been invaded the right to submit a complaint to national courts.

¹¹⁴ James Woolsey (former CIA Director), *Why America Spies on its Allies*, *The Wall Street Journal Europe*, 22 March 2000, 31, and Remarks at the Foreign Press Centre, transcript, 7 March 2000, <http://cryptome.org/echelon-cia.htm>.

¹¹⁵ Article 8(2) of the ECHR lays down these issues as grounds justifying interference in an individual's exercise of the right to privacy.

¹¹⁶ British law is an exception, giving the Home Secretary the power to issue authorisations (Regulation of Investigatory Powers Act 2000, Section 5(1) and (3)(b)).

¹¹⁷ For example, in Austria and Belgium.

¹¹⁸ For example, in Germany, law on the restriction of post and telecommunications secrecy (Law on Article 10 of the Basic Law). Pursuant to paragraph 9, except in cases where there is a risk that delay would frustrate the operation, the commission must be informed before the surveillance is carried out.

¹¹⁹ For example in the United Kingdom (Regulation of Investigatory Powers Act, Section 1), and in France for cable communications (Law 91/646 of 10 July 1991 *CE loi relative au secret des correspondances émises par la voie de télécommunications*).

¹²⁰ For example cable communications in France (Article 20 of Law 91/646 of 10 July 1991 - *loi relative*

au secret des correspondances émises par la voie de télécommunications).

¹²¹ For full details see ‘The Parliamentary Supervision of the Intelligence Services in Germany, as at 9.9.2000’, published by the German Bundestag, Secretariat of the Parliamentary Control Body.

¹²² Law on the supervision of federal intelligence activities (PKGrG) of 17 June 1999, BGBl I 1334 idgF.

¹²³ Law 91-646 of 10 July 1991; loi relative au secret des correspondances émises par la voie de télécommunications.

¹²⁴ See the Bill entitled ‘Proposition de loi tendant à la création de délégations parlementaires pour le renseignement’, and the related report by *Arthur Paecht*, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N o 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d’une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de L’Assemblée nationale le 23 novembre 1999.

¹²⁵ Intelligence Services Act 1994, Section 10

¹²⁶ Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 / IV, organique du contrôle des services de police et de renseignements.

¹²⁷ Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarrets og politiets efterretningsjenester, lov 378 af 6.7.88.

¹²⁸ Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) vom 17 Juni 1999 BGBl I 1334 idgF.

¹²⁹ Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento de servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

¹³⁰ Tweede-Kamercommissie voor de Inlichtingen-en Veiligheidsdiensten, 17. Reglement van order van de Tweede Kamer der Staten-Generaal, Art. 22.

¹³¹ Conselho de Fiscalização dos Serviços de Informações (CFSI), Law 30/84 of 5.9.1984, amended by Law 4/95 of 21.2.1995, Law 15/96 of 30.4.1996 and Law 75-A/97 of 22.7.1997.

¹³² Intelligence and Security Committee (ISC), Intelligence Services Act 1994, Section 10.

¹³³ Standing Subcommittee of the National Defence Committee responsible for monitoring intelligence measures to safeguard military security and the Standing Subcommittee of the Committee on Internal Affairs responsible for monitoring measures to protect constitutional bodies and their ability to act, Article 52a B-VG, §§ 32b et seq., Law on the Rules of Procedure,

1975.

¹³⁴ Ombudsman, legal basis for supervision of the police (SUPO): Poliisilaki 493/1995 § 33 and Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 § 15, for the military: Poliisilaki 493/1995 § 33 and Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 § 5.

¹³⁵ Rikspolisstyrelsens ledning, Förordning (1998: 773) med instruktion för Rikspolisstyrelsen (Regulation (1989: 773) on the national police authority).

¹³⁶ Information for firms provided with security protection, Federal Ministry of Economic Affairs, 1997.

¹³⁷ Michael E. Porter, *Competitive Strategy*, Simon & Schuster (1998). 206 *Roman Hummelt*, *Industrial espionage on the data highway*, Hanser Verlag (1997). 207 Details and names confidential.

¹³⁸ *Impulse*, 3/97, 13 et seq.

¹³⁹ Louis J. Freeh, Director FBI, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996.

¹⁴⁰ Robert Lyle, *Radio Liberty/Radio Free Europe*, 10.2.1999.

¹⁴¹ *Computerzeitung*, 30.11.1995, 2.

¹⁴² *Roman Hummelt*, *Spionage auf dem Datenhighway*, Hanser Verlag (1997), 49 et seq

¹⁴³ Confidential statement to the reporter by a counterintelligence service, source protected.

¹⁴⁴ State Department Foreign Press Center briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000.

¹⁴⁵ Statement for the Record of *Louis J. Freeh*, FBI Director, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996.

¹⁴⁶ The end of the Cold War has not resulted in a peace dividend regarding economic espionage, Statement for the Record of *Louis J. Freeh*, FBI Director, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996.

¹⁴⁷ Interpretation by your reporter of the cryptic remarks made by *Louis J. Freeh* to the committee.

¹⁴⁸ In these areas the interception of communications is a promising method!

¹⁴⁹ James Woolsey, Remarks at the Foreign Press Center, Transcript, 7.3.2000, <http://cryptome.org/echelon-cia.htm>.

¹⁵⁰ As I indicated also in my testimony, there are instances where we learn, that foreign companies or their governments bribe, lie, cheat or steal their way to disenfranchise American companies. When we generate this information, we take it to other appropriate

agencies, make them aware of it. They use that information through other means and channels to see if they can assist an American company. But we play defense, we never play offense, and we never will play offense.

¹⁵¹ Albin Eser, Michael Überhofer, Barbara Huber (Eds), Using the criminal law to combat corruption. A comparative survey of offences involving bribery, drawn up on behalf of the Bavarian Ministry of Justice, edition iuscrim (1997).

¹⁵² The scale runs from 10 (low incidence of bribery) to 0 (high incidence of bribery): Sweden (8.3), Australia (8.1), Canada (8.1), Austria (7.8), Switzerland (7.7), Netherlands (7.4), United Kingdom (7.2), Belgium (6.8), Germany (6.2), USA (6.2), Singapore (5.7), Spain (5.3), France (5.2), Japan (5.1), Malaysia (3.9), Italy (3.7), Taiwan (3.5), South Korea (3.4) and China (3.1). <http://www.transparency.org/documents/cpi/index.html#bpi>.

¹⁵³ OFFICE OF THE CHIEF COUNSEL FOR INTERNATIONAL COMMERCE, Legal Aspects of International Trade and Investment, <http://www.ita.doc.gov/legal/>

¹⁵⁴ <http://www.oecd.org/daf/nocorruption/annex3.htm>.

¹⁵⁵ Criminal Law Convention on Corruption <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=173&CM=8&DF=21/06/01>

¹⁵⁶ Civil Law Convention on Corruption ETS no.: 174, <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=174&CM=8&DF=21/06/01>

¹⁵⁷ Convention, drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union, on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, OJ C 195, 25.6.1997, 2.

¹⁵⁸ Joint Action of 22 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on corruption in the private sector (98/742/JHA), OJ L 358, 31.12.1998, 2.

¹⁵⁹ White House Archive, <http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html>.

¹⁶⁰ Homepage of the National Security Council (NSC), <http://www.whitehouse.gov/nsc>.

¹⁶¹ TPCC brochure on the Advocacy Center, October 1996.

¹⁶² Homepage of the Advocacy Center, <http://www.ita.doc.gov/td/advocacy/>

¹⁶³ TPCC Working Group Meeting, Agenda, 18.7.1994, TPCC Indonesia Advocacy-Finance Working Group, Distribution List, and Minutes of the meeting of 17.8.1994, from a letter from the US and Foreign Commercial Service of 25.8.1994.

¹⁶⁴ *ibidem*: 'Bob Beamer suggested that any primary

competitors known to the group for these projects should be included as background information', Bob Beamer is one of the CIA representatives.

¹⁶⁵ Computer espionage, Document 44, Federal Ministry for Economic Affairs, July 1998.

¹⁶⁶ Roman Hummelt, Industrial Espionage on the Data Highway, Hanser Verlag (1997).

¹⁶⁷ George Kurtz, Stuart McClure, Joel Scambray, Hacking exposed, Osborne/McGraw-Hill (2000), 94.

¹⁶⁸ Martin Kuppinger, Internet and Internet Security, Microsoft Press Deutschland (1998), 60.

¹⁶⁹ Othmar Kyas, Security on the Internet, International Thomson Publishing (1998), 23.

¹⁷⁰ Anonymous, Hacker's guide, Markt & Technik-Verlag (1999).

¹⁷¹ Information supplied by members of COREPER [The Committee of Permanent Representatives of the Member States of the European Union] and Council officials; sources protected.

¹⁷² Council Decision of 19 March 2001 adopting the Council's security regulations, OJ L 101, 11.4.2001, 1.

¹⁷³ There is evidence of this even in antiquity, e.g. the use of the *skytale* or cipher rod by the Spartans in the 5th century BC.

¹⁷⁴ Otto Leiberich, , Vom diplomatischen Code zur Falltürfunktion ¶ Hundert Jahre Kryptographie in DeutschlandTM [From diplomatic code to trap-door function ¶ a hundred years of cryptography in Germany], *Spektrum der Wissenschaft* June 1999, 26 et seq.

¹⁷⁵ It was introduced by Major Joseph Mauborgne, head of the cryptographic research division of the American army; Simon Singh, *The Code Book* (1999), Carl Hanser Verlag 151.

¹⁷⁶ Simon Singh, *The Code Book* (1999), Carl Hanser Verlag 151 et seq.

¹⁷⁷ Reinhard Wobst, *Abenteuer Kryptologie 2*, Adison-Wesley (1998), 60.

¹⁷⁸ Enigma was developed by Arthur Scherbius and patented in 1928. It was a little like a typewriter, as it had a keyboard on which the plain text was keyed in. By means of a peg-board and rotating drums the text was encoded in accordance with given rules and decoded at the other end on the same machine using code books.

¹⁷⁹ American Standard Code for Information Exchange.

¹⁸⁰ A= 1000001, B= 1000010, C=1000011, D=1000100, E= 1000101, etc.

¹⁸¹ In binary terms, this number consists of 56 zeros and ones. See Singh, *The Code Book*, Carl Hanser Verlag (1999), 303.

¹⁸² Simon Singh, *The Code Book*, Carl Hanser Verlag (1999), 302 et seq.

¹⁸³ It was created by two Belgian cryptographers working

at the Catholic University of Louvain, Joan Daemen and Vincent Rijmen.

¹⁸⁴ The idea of asymmetric encryption using the public-key process was devised by Whitfield Diffie and Martin Hellmann.

¹⁸⁵ Simon Singh, *The Code Book*, Carl Hanser Verlag (1999), 327.

¹⁸⁶ Johannes Buchmann, *Factoring large integers*, *Spektrum der Wissenschaft* 2, 1999, 6 et seq.

¹⁸⁷ Simon Singh, *The Code Book*, Carl Hanser Verlag (1999), 335 et seq.

¹⁸⁸ Information on the software can be found at www.pgpi.com.

¹⁸⁹ On quantum cryptology, see Reinhard Wobst, *Abenteuer Kryptographie 2*, Adison-Wesley (1998), 224 et seq.

¹⁹⁰ Charles Grant, *Intimate relations. Can Britain play a leading role in European defense - and keep its special links to US intelligence?* 4.2000, Centre for European Reform.

George and Marisol Gari

The FBI arrested two additional members of the Cuban “La Red Avispa”—the Wasp Network—on 31 August 2001. Taken into custody by the FBI in Orlando, Fla., were George Gari and his wife, Marisol, for trying to infiltrate Cuban exile and US military installations. George was born in Brooklyn, N.Y., but moved to Cuba as a child.

In the three-count indictment, George, 40, and his wife, 42, were charged with conspiracy to act as agents of a foreign government without proper identification or notice to the attorney general. The FBI said that the espionage by the Garis occurred between 1991 and 1998 and that Marisol used her US Postal Service job to gain access to mail sent by and intended for Cuban Americans. She also compiled a report on various US mail systems for her Cuban bosses.

The Garis also are suspected of conducting surveillance on the Cuban American National Foundation, including surveying the interior layout and the security measures in place at the Foundation’s Miami headquarters. According to the FBI, George, who worked for Lockheed Martin, was ordered by his Cuban handlers to apply for work at the Southern Command but was unsuccessful.

Known by the codenames “Luis” and “Margot,” authorities said the Garis received training by the Cuban Directorate of Intelligence (DI) before their 1990 arrival in the United States and, together, used advanced encryption technology to transmit information about anti-Castro exile organizations between the Cuban Government and other agents.

A federal grand jury sitting in Miami, Florida, returned a three-count Indictment charging George and Marisol with spying for the Government of Cuba.

As set forth in the indictment, the object of the conspiracy was that the defendants and their co-conspirators would function as covert spies serving the interests of the government of the Republic

of Cuba within the United States. Their task was to gather and transmit information to the Cuban Government concerning US Government functions and installations by informing on anti-Castro Cuban political groups in Miami-Dade County and by carrying out other operational directives of the Cuban Government.

As set forth in the indictment, trained officers of the Cuban DI, known as illegal officers, would take up residence in South Florida and carry out clandestine activities on behalf of the Cuban Government. These officers would manage and oversee the activities of agents, transmitting to the agents instructions received by the illegal officers from the Republic of Cuba. The illegal officers also would receive oral and recorded reports from the agents and cause these reports to be communicated to the Republic of Cuba.

The network of Miami-based illegal officers and agents was known as La Red Avispa and their activities were overseen, directed, analyzed, and reviewed by the DI in Cuba. The illegal officers would and did receive and transmit to the agents instructions, which the agents would and did carry out, to conduct covert and clandestine activities on behalf of the Republic of Cuba.

On 20 September 2001, the Garis pleaded guilty to spying for Cuba, but Marisol's plea occurred behind closed doors. Her plea agreement, which was sealed by the US District Judge, called for her to cooperate with federal prosecutors in their continuing investigation. Marisol's lawyer confirmed that she pleaded guilty to one count of conspiracy to act as an unregistered agent for Cuba. She faces a maximum of five years in prison and could be deported afterward because she is not a US citizen. In turn, prosecutors dropped a second charge of acting as an unregistered Cuban agent, which carried a 10-year sentence.

After Marisol made her plea, the courtroom was reopened for George's guilty plea to one count of acting as an unregistered agent for Cuba. He faces a maximum of 10 years. In return, prosecutors agreed to recommend a reduction in his sentence

and dropped a second charge of conspiracy. His plea agreement does not call for him to cooperate.

Many of the lawyers for the high-ranking Cuban La Red Avispa spies said that the Garis were relatively low-level functionaries in the network and did not believe that they would have any important information to provide to US authorities. However, because they reported to several of the higher-ranking Cuban DI illegal agents and had started "handling" other spies, according to the plea agreements, they may be able to shed additional light on the Cuban network and possibly other members still at large.

On 4 January 2002, George and Marisol Gari received prison sentences of seven years and three and a half years, respectively.

Japan

Japan is cited as a good example of a country whose government has played a key role in collecting, analyzing, and disseminating foreign technology information to both its industry and government. In the early part of the 20th century, Japan's foreign technical collection was done by some of its corporations, which had worldwide intelligence networks. However, the real boom came after the allied occupation in 1945, when former military intelligence officers found new homes for their skills in Japan's consolidated trading companies. After World War II, Japan also solidified its technology base by importing foreign technology to supplement its own research and development efforts.

Japan's primary industrial technology agency is the Ministry of International Trade and Industry (MITI). MITI's mission is to further industrial research and development in Japan, and it has been the engine of Japan's economic miracle since its founding in 1949.

Japanese research and development capabilities have grown, and Japanese Government industrial policies continue to target knowledge-intensive technologies as well as substantially increasing government and industry investments in new technologies.² Many Japanese technological capabilities now match those of the United States and in some cases have surpassed US capabilities.

The Japanese Government has an extensive, centrally coordinated process and uses considerable resources to collect and disseminate foreign technology information primarily for commercial purposes. This process is characterized by extensive networks between officials and researchers in government, industry, and academia that provide information and a methodical process of consensus building regarding what technologies should be monitored within a competitive, commercial framework. Experts collect information in specific areas of interest, which is targeted to the needs of the users, and then use extensive and multiple channels to disseminate the

data. MITI facilitates and coordinates government, industry, and academic activities, including research and development programs and foreign technology information collection efforts, by providing technology information and significant funding for these activities.

Japanese Government and private-sector officials stressed the importance of determining and providing the foreign technology information that customers want and need. Other elements of a successful system that they identified include maintaining a cooperative government-industry relationship, treating technology monitoring as an integral part of an organization's operations, and locating operations in the target country.

The Japanese Government plays a more significant and intense role in guiding the national research and development effort for economic competitiveness. In addition, Japan spends a lot of money to collect, analyze, and disseminate foreign technology information to its government, industry, and academia.

MITI retains its reputation abroad as being the headquarters of "Japan Incorporated." With its 15,000 employees, MITI has no counterpart in the United States or in most other industrialized nations. MITI's role as a government ministry is to work closely with private industry to identify strategic markets and products.

MITI establishes organizations that carry out specific research and development programs. It provides funds (subsidies) and/or information, such as data on foreign technology policy and research capabilities, to government and private-sector organizations for research and development projects. It also coordinates government-industry policies, for example, by routing information toward those who will benefit from it and facilitates technology diffusion and transfer.

One organization that has changed its mission is the Asian Office of Aerospace Research and Development. The mission of the Asian Office, which was reestablished in Tokyo, was changed

to include monitoring more applied technology, which may be useful to industry, as well as the basic technology on which they have traditionally focused.

Despite its industry orientation, MITI has been likened to a military intelligence service, choosing targets based on the basis of national interest and coordinating collection. For example, in 1976 MITI set up a Committee on Information and Acquisitions in its Electrotechnical Laboratory to monitor developments in the US computer industry. Funds were available to purchase information from individuals in the United States who were willing to sell it, whether legally or illegally, through front companies set up by MITI or by way of consulting contracts with employees of US computer firms.

This information was instrumental in Japan's subsequent ability to dominate the field of microelectronics. Since the 1980s, MITI has been running the same type of operation against the US biotech and aerospace industries.

The Japanese Government primarily collects foreign technology information through MITI-sponsored organizations. In response to requests from government organizations, industry, and academia, the Japan External Trade Organization (JETRO), MITI's primary information collection organization, collects foreign technology information through its extensive network of offices in Japan and overseas and disseminates it to requesters.

Because of the cozy relationship between MITI and industrialists, Japan established an impressive collection system. JETRO is its key organization, but all Japan's services abroad and all individuals on foreign travel, whether for professional purposes or not, were part of it. The system's strength is in the "symbiosis between state and industry and in the overall consensus on the pooling of information."³

The role of JETRO in collecting foreign intelligence is legendary. Created in 1958 as part of MITI's International Trade Administrative

Bureau to support foreign trade, JETRO's unofficial major task has been to collect intelligence on foreign business strategies, trade secrets—now illegal under the Economic Espionage Act of 1997—and new technologies. Overall, JETRO has 1,300 staff in a total of 79 offices worldwide, seven of which are in the United States—Atlanta, Chicago, Denver, Houston, Los Angeles, New York, and San Francisco.

Despite these government efforts, many Japanese Government officials and industry representatives said that Japanese companies are the primary collectors of specific information on foreign technologies.⁴ This is true particularly for large firms, such as Nippon Electronics Corporation, that have extensive, in-house capabilities to monitor and disseminate foreign technology information within the company. Japanese businessmen are voracious consumers of technical information. In addition, the Japanese Government and private sector have relatively easy access to US technology information because many Japanese, including scientists and engineers, speak and read English, and much of the US research and development is done in an open university system.

A typical trading company collects about 100,000 pieces of information from its 10,000 plus employees in about 180 offices worldwide and spends over \$60 million annually to maintain its collection infrastructure. Many overseas branches of Japanese companies are located near high-technology centers, which in the United States include Silicon Valley, the Route 128 corridor in Massachusetts, the Rockville area of Maryland, and Northern Virginia.

Besides helping Japan keep up with the latest developments in technology, their strategic locations facilitate negotiation of joint ventures with high-tech and capital-starved US startups as a means of acquiring promising new technology. It also allows direct recruitment of local scientists, technical experts, and employees of competing firms with inside knowledge of that firm's technology.

Japan does recruit human sources but unlike Western intelligence services that recruit individuals to spy against their organization, Japan uses two other methods. The first is a vigorous hiring campaign conducted by Japanese companies in sectors judged by MITI and the companies themselves to be of importance. For example, in one issue of an industry magazine, Toshiba America Electronics Components, Inc., a Silicon Valley subsidiary of the Japanese electronics manufacturers, ran an advertisement asking US semiconductor engineers with three or more years experience to become part of “the new wave of VLSI technology.” A few pages later, Fujitsu Microelectronics in San Jose, California, invited experienced computer engineers to “imagine a world without any boundaries.” The ad promised that, “We’re not about to put limits on your creativity either.” In the same issue, HAL Computer Systems, another Fujitsu subsidiary in Silicon Valley, tried to interest US software engineers in joining “The Dawn of a New Era.”

The second technique used is where Japanese employees of local subsidiaries seek personal relationships with specialists at nearby US companies who are in a position to provide technical information. Occasionally, these efforts to suborn US employees are detected. An example of this occurred when Hitachi and Mitsubishi Electric tried to obtain proprietary technology illegally from an IBM employee through a Silicon Valley-based consulting company. In another exposed operation, Japanese agents in San Francisco recruited a mid-level engineer at Fairchild, who between 1977 and 1986 passed some 160,000 pages of research results to the consultants of Japanese companies.

An effective addition to the above methods is Japan’s extensive use of travelers to collect information. Japanese companies have a history of sending individual businessmen abroad on technology-gathering missions. The effort began in the 1950s with government-subsidized expeditions primarily to the United States to scout out and obtain new technologies. It continues today with as many as 10,000 trips annually reported. Collection

goals can be generic or technology specific. Also important are the 15,000 plus Japanese scientists and engineers staying in the United States at high-tech companies or US Government-funded laboratories under exchange programs or “co-development” projects.

Representatives of Japanese organizations attend symposiums and international conferences, collect technical literature, and visit laboratories and individual scientists. Japanese officials emphasized that it was useful to establish and maintain informal networks with other Japanese and foreign scientists. Japanese officials use journals, reports, newsletters, databases, facsimiles, the Internet, and workshops to disseminate information.

Japanese Government and private-sector officials cited four elements that they believe contribute to a successful system for collecting and disseminating foreign technology information. They are targeted data collection, a cooperative government-industry relationship, treatment of foreign technology monitoring as an integral part of their operations, and establishment of operations in the target country.

One important element of an effective information collection and dissemination effort cited by the Japanese is that it be demand driven. In other words, the needs of the users of the information must be identified and met for the collection to be successful. For example, JETRO regularly uses inquiries to survey its customers’ needs and determine the best dissemination method. JETRO, among other activities, gathers information for private companies on technologies and markets based on specific requests for information, in much the same way that a consulting company would tailor information to a client’s strategic and operational needs.

According to Japanese officials, the Japanese Government and industry have a very effective government-industry relationship that contributes to the flow of foreign technology information among various organizations. In addition, Japanese company officials said that one of their most useful

methods of obtaining information is participating in government-sponsored research and development projects where several Japanese companies are involved.⁵

A State Department official said that there is a more cooperative government-industry relationship in Japan than in the United States because the Japanese Government does not restrict the flow of information to the private sector. He said that the Japanese Government has fewer security and copyright restrictions on information due to its more informal process of disseminating information. For example, the Japanese Government provides information to Japanese industry associations that condense and repackage the information.

Another effective element cited by the Japanese is that those organizations treat foreign technology monitoring as an integral part of their operations. Rather than having separate, specific offices for this activity, researchers, scientists, and others throughout the organizations monitor foreign technology information. For example, the Japanese research and development consortium for superconductor technology expects all its researchers to stay abreast of foreign technology developments in their field as part of their work

Endnotes

¹ Much of the information in this article comes from a Government Accounting Office report, "Foreign Technology: Collection and Dissemination of Japanese Information Can Be Improved," GOA/NSIAD-93-251, 30 September 1993. It has been updated with additional information.

² *Japan-U.S. Economic Issues: Investment, Saving, Technology, and Attitudes*, Congressional Research Office, 2 February 1990.

³ Jean-Francois Daguzan, "From Intelligence to Lobbying," *Paris Le Nouvel Economiste*, 18-31 May 2001.

⁴ Japan also has networks of related companies and financial institutions called *keiretsu* that provide means for information exchange as well as risk sharing and mutual problem solving. See *Competitiveness Issues: The Business Environment in the United States, Japan, and Germany* (GAO/GGD-93-124, August 9, 1993).

⁵ Officials from a US company said that foreign technology information is also obtained from negotiating a coproduction agreement, even when the company decides not to do the project. Coproduction is overseas production based on government-to-government agreement that permits a foreign government or producer to acquire the technical information to manufacture all or part of a US-origin defense article.

Background

The South Korean National Assembly easily elected Syngman Rhee president in 1948, but almost immediately, Rhee ran into difficulties. Most of Rhee's efforts during his time in office (1948-60) involved his own personal struggle to stay in power against his opponents trying to unseat him. Constitutional provisions concerning the presidency became the focal point.

The South Korean constitution called for a four-year term limit on the presidency. Because Rhee had little prospect of being reelected by the National Assembly, he tried to get a constitutional amendment passed in the National Assembly in November 1951 to elect the president by popular vote. This proposal was resoundingly defeated by a vote of 143 to 19, prompting Rhee to marshal his supporters in the Liberal Party. Four months later, in April 1952, the opposition introduced another motion calling for a parliamentary form of government. In response, Rhee declared marshal law in May, rounded up the assembly members by force, and called for another vote. His constitutional amendment to elect the president by popular vote was railroaded through, passing with 163 votes of the 166 assembly members present. In the subsequent popular election in August 1952, Rhee was reelected by 72 percent of the voters.

The constitution, however, limited the president to only two terms. Hence, when the end of Rhee's second term of office approached, the constitution again was amended in November 1954 by the use of fraudulent tactics that allowed Rhee to succeed himself indefinitely.

In the meantime, South Koreans—particularly the urban masses—had become more politically astute. The press frequently exposed government ineptitude and corruption and attacked Rhee's authoritarian rule. The Democratic Party capitalized on these issues, and in the presidential election of May 1956, Rhee won only 55 percent of

the votes, even though his principal opponent—Sin Ik-hui—had died of a heart attack ten days before the election. Rhee's running mate, Yi Ki-bung, fared much worse, losing to the Democratic Party candidate, Chang Myon (John M. Chang). Since Rhee was already 81 years old in 1956, Chang's victory caused a major tremor among Rhee's supporters.

Thereafter, the issue of Rhee's age and the goal of electing Yi Ki-bung became an obsession. The administration became increasingly repressive as Liberal Party leaders came to dominate the political arena, including government operations, around 1958. Formerly Rhee's personal secretary, Yi and his wife (Mrs. Rhee's confidant and a power behind the scenes) had convinced the childless Rhee to adopt their son as his legal heir. For fear that Rhee's health might be impaired, he was carefully shielded from all information that might upset him. Thus, the aged and secluded president became a captive of the system he had built, rather than its master.

In March 1960, the Liberal Party managed to reelect Rhee and to elect Yi Ki-bung vice president by the blatant use of force. Rhee was reelected by default because his principal opponent had died while receiving medical treatment in the United States just before the election. As for Yi, he was largely confined to his sickbed—a cause of public anger—but won 8.3 million votes as compared to 1.8 million votes for Chang Myon. The fraudulent election touched off civil disorders, known and celebrated as the April 19 Student Revolution, during which the police killed 142 students. As a result, Rhee resigned on 26 April 1960. The next day, all four members of Yi's family died in a suicide pact. This account has been challenged by some who believe Yi's bodyguards killed the family in hopes of enabling Rhee to stay on.

Rhee's resignation left a political void subsequently filled by Ho Chong, whom Rhee had appointed foreign minister the day before he resigned. Although Ho was a lifelong friend of Rhee, he had maintained amicable relations with Democratic Party leaders and was acceptable to all concerned.

Between April and July 1960, Ho's transitional government maintained order, exiled Rhee and his wife to Hawaii, and prepared for a new general election of the National Assembly in July. The transitional government revised the constitution on 15 June, instituting a parliamentary form of government with a bicameral legislature. In the election of July 1960, the Democratic Party won 175 of the 233 seats in the lower house of the National Assembly. The second-largest group, the independents, won 49 seats. The Liberal Party won only two seats. In the upper house, the Democratic Party won 31 of the 58 seats.

The Democratic Party had been a coalition of two divergent elements that had merged in 1955 to oppose Rhee. When the common enemy—Rhee and his Liberal Party—had been removed from the scene and opportunities for power were presented, each group sought to obtain the spoils for itself.

The Democratic Party candidate for the presidency in the March 1960 election, Cho Pyong-ok, died of illness shortly before the election, just as his predecessor, Sin Ik-hui, had in 1956. The two divergent Democratic Party groups openly struggled against each other during the elections in July for the National Assembly. Although they agreed on Yun Po-son as presidential candidate and Chang Myon as their choice for premier, neither had strong leadership qualities nor commanded the respect of the majority of the party elite. During its brief eight-month term—beginning October 1960—a parliamentary-cabinet system was introduced similar to that which exists in the United Kingdom, and efforts were made to decentralize and curb the powers of the executive. Yun and Chang could not agree on the composition of the cabinet. Chang attempted to hold the coalition together by reshuffling cabinet positions three times within a five-month period. In November 1960, the group led by Yun left the Democratic Party and formed the New Democratic Party.

In the meantime, the tasks confronting the Chang's new government were daunting. The economy suffered from mismanagement and corruption. The army and police needed to be purged of

the political appointees who had buttressed the dictatorship. The students, to whom the Democratic Party owed its power, filled the streets almost daily, making numerous wide-ranging demands for political and economic reforms, but the Democratic Party had no ready-made programs. Law and order could not be maintained because the police, long an instrument of the Rhee government, were demoralized and totally discredited by the public. Continued factional wrangling caused the public to turn away from the party.

This situation provided a fertile ground for a military coup. Rhee had been able to control the military because of his personal prestige, his skill in manipulating the generals, and the control mechanisms he had instituted; Chang lacked all these advantages. When the demands of the young army officers under Maj. Gen. Park Chung Hee were rebuffed, and as political power appeared to be increasingly hanging in the balance with no one clearly in charge, the army carried out a coup d'état on 16 May 1961. Chang's own army chief of staff, Chang To-yong, joined the junta, and Chang Myon's fragile government was toppled. (The junta subsequently tried and convicted General Chang for attempting to take over the junta.) The young officers' initial complaint had been that Chang Myon had not kept a campaign pledge to weed out corrupt generals from the South Korean army, and some Korean sources attributed this failure to the intervention of high-ranking US military officers, who feared the weakening of South Korea's national security.

Yun Po-son, leader of the New Democratic Party, sided with the junta and persuaded the US Eighth Army and the commanders of various South Korean army units not to interfere with him and his party. Yun stayed on as president for ten months after the military junta seized power, thereby legitimizing the coup. A small number of young officers commanding 3,600 men had succeeded in toppling a government with authority over an army of 600,000.

The junta under Maj. Gen. Park Chung Hee quickly consolidated its power, removed those it considered

corrupt and unqualified from government and army positions, and laid plans for the future. The 32-member Supreme Council for National Reconstruction became all powerful.

The Creation of the Korean Central Intelligence Agency

The Korean Central Intelligence Agency (KCIA) was originally established on 19 June 1961 to prevent a countercoup and to suppress all potential enemies. Its duties were to “supervise and coordinate both international and domestic intelligence activities and criminal investigation by all government intelligence agencies, including that of the military.” The KCIA had the power to arrest and detain anyone suspected of wrongdoing or harboring antijunta sentiments. Its mission was akin to that of a combined US Central Intelligence Agency and Federal Bureau of Investigation.

The first head of the KCIA was Kim Chong-p’il. Kim utilized the existing Army Counterintelligence Corps to build a 3,000-member organization—the most powerful intelligence and investigative agency in the republic. The KCIA maintained a complex set of interlocking institutional links to almost all of the government’s key decisionmaking bodies. The KCIA had a near monopoly over crucial information concerning national security under the charter of the Act Concerning Protection of Military Secrets and, more important, possessed considerable veto power over other agencies through its supervisory and coordination functions.

The KCIA’s practically unlimited power to investigate and to detain any person accused of antistate behavior severely restricted the right to dissent or to criticize the regime. The frequent questioning, detention, or even prosecution of dissidents, opposition figures, and reporters seriously jeopardized basic freedoms and created an atmosphere of political repression.

Under Park, the lack of advancement in civil liberties continued to be justified by referring to the threat from North Korea. The political influence

of the Ministry of Home Affairs and the police declined in the face of the KCIA’s power. The relationship between the police and general public, however, was not significantly altered. As Se-Jin Kim wrote in 1971: “The former still act with arbitrary arrogance; the latter respond with fear but not respect.”

The government often used martial law or garrison decree in response to political unrest. From 1961 to 1979, martial law or a variant was evoked eight times. The garrison decree of 15 October 1971, for example, was triggered by student protests and resulted in the arrest of almost 2,000 students. A year later, on 17 October 1972, Park proclaimed martial law, disbanded the National Assembly, and placed many opposition leaders under arrest. In November, the *yusin* constitution (*yusin* means revitalization), which greatly increased presidential power, was ratified by referendum under martial law.

The government grew even more authoritarian, governing by presidential emergency decrees in the immediate aftermath of the establishment of the *yusin* constitution; nine emergency decrees were declared between January 1974 and May 1975. The Park regime strengthened the originally draconian National Security Act of 1960 and added an even more prohibitive Anticommunism Law. Under those two laws and Emergency Measure Number Nine, any kind of antigovernment activity—including critical speeches and writings—was open to interpretation as a criminal act of “sympathizing with communism or communists” or “aiding antigovernment organizations.” Political intimidation, arbitrary arrests, preventive detention, and brutal treatment of prisoners were not uncommon.

Opposition to the government and its harsh measures increased as the economy worsened in 1979. Scattered labor unrest and the government’s repressive reactions sparked widespread public dissent resulting in mass resignation of the opposition membership in the National Assembly and student and labor riots in Pusan, Masan, and Ch’angwon. The government declared martial law

in the cities. In this charged atmosphere and under circumstances that appeared related to dissatisfaction with Park's handling of the unrest, on 26 October 1979, KCIA chief Kim Chae-gyu killed Park and the chief of the Presidential Security Force—Ch'a Chi-ch'ol—and then was himself arrested. [The nominal Prime Minister Ch'oe Kyo-ha became president.] Emergency martial law was immediately declared to deal with the crisis, placing the head of the Defense Security Command—Maj. Gen. Chun Doo Hwan—in a position of considerable military and political power.

After the assassination in 1979 of President Park by the KCIA director, the KCIA was purged and temporarily lost much of its power. Chun Doo Hwan used his tenure as acting director of the KCIA from April to July 1980 to expand his power base beyond the military. The slow pace of reform led to growing popular unrest. In early May 1980, student demonstrators protested a variety of political and social issues, including the government's failure to lift emergency martial law imposed following Park's assassination. The student protests spilled into the streets, reaching their peak during the period 13 to 16 May, at which time the student leaders obtained a promise that the government would attempt to speed up reform. The military's response, however, was political intervention led by Lt. Gen. Chun Doo Hwan, then KCIA chief and army chief of staff. Chun had forced the resignation of Ch'oe's cabinet; banned political activities, assemblies, and rallies; and arrested many ruling and opposition politicians. In Kwangju, demonstrations to protest the extension of martial law and the arrest of Kim Dae Jung—the leading opposition candidate who later became president on 18 December 1997—turned into rebellion as demonstrators reacted to the brutal tactics of the Special Forces sent to the city. The government did not regain control of the city for nine days, after some 200 deaths.

Agency for National Security Planning

The KCIA was renamed the Agency for National Security Planning (NSP), and its powers were

redefined in presidential orders and legislation. The NSP, like its predecessor, was a cabinet-level agency directly accountable to the president. The director of the NSP continued to have direct presidential access. In March 1981, the NSP was redesignated as the principal agency for collecting and processing all intelligence. The requirement for all other agencies with intelligence-gathering and analysis functions in their charters to coordinate their activities with the NSP was reaffirmed.

Legislation passed at the end of 1981 further redefined the NSP's legally mandated functions to include the collection, compilation, and distribution of foreign and domestic information regarding public safety against communists and plots to overthrow the government. The maintenance of public safety with regard to documents, materials, facilities, and districts designated as secrets of the state was the purview of the NSP. Also under NSP's authority was the investigation of crimes of insurrection and foreign aggression, crimes of rebellion, aiding and abetting the enemy, disclosure of military secrets, and crimes provided for in the Act Concerning Protection of Military Secrets and the National Security Act. The investigation of crimes related to duties of intelligence personnel, the supervision of information collection, and the compilation and distribution of information on other agencies' activities designed to maintain public safety also were undertaken by the NSP. By 1983, the NSP had rebounded and again was the preeminent foreign and domestic intelligence organization.

Public discontent was kept under control until 1987 by the regime's extensive security services—particularly the Agency for National Security Planning, the Defense Security Command (DSC), and the Combat Police of the Korean National Police (KNP). Both the civilian NSP and the military DSC not only collected domestic intelligence but also continued “intelligence politics.” The Act Concerning Assembly and Demonstration was used to limit the expression of political opposition by prohibiting assemblies likely to “undermine” public order. Advanced

police notification of all demonstrations was required. Violation of the act carried a maximum sentence of seven years' imprisonment or a fine. Most peaceful nonpolitical assemblies took place without government interference. However, the act was the most-frequently-used tool to control political activity in the Fifth Republic, and the Chun regime was responsible for more than 84 percent of the 6,701 investigations pursued under the act.

The security presence in city centers, near university campuses, government and party offices, and media centers was heavy. Citizens, particularly students and young people, were subject to being stopped, questioned, and searched without due process. The typical response to demonstrations was disruption by large numbers of Combat Police, short-term mass detention of demonstrators, and selective prosecution of the organizers. Arrest warrants—required by law—were not always produced at the time of arrest in political cases.

The National Security Act increasingly was used after 1985 to suppress domestic dissent. Intended to restrict “anti-state activities endangering the safety of the state and the lives and freedom of the citizenry,” the act also was used to control and punish nonviolent domestic dissent. Its broad definition of offenses allowed enforcement over the widest range, wider than that of any other politically relevant law in South Korea. Along with other politically relevant laws such as the Social Safety Act and the Act Concerning Crimes Against the State, the National Security Act weakened or removed procedural protection available to defendants in nonpolitical cases.

Questioning by the security services often involved not only psychological or physical abuse but also outright torture. The torture and death of Pak Chong-ch'ol in 1987, a student at Seoul National University being questioned as to the whereabouts of a classmate, played a decisive role in galvanizing public opposition to the government's repressive tactics.

The security services not only detained those accused of violating laws governing political

dissent but also put under various lesser forms of detention—including house arrest—those people, including opposition politicians, who they thought intended to violate the laws. Government agents subjected many political, religious, and other dissidents to surveillance. Opposition assembly members later charged in the National Assembly that telephone tapping and the interception of correspondence were prevalent. Ruling party assembly members, government officials, and senior military officials probably also were subjected to this interference although they did not openly complain.

Use of tear gas by the police (more than 260,000 tear gas shells were used in 1987 to quell demonstrations) increasingly was criticized. The criticism eventually resulted in legal restrictions on tear gas use in 1989. The government continued, however, to block many “illegal” gatherings organized by dissidents that were judged to incite “social unrest.” In 1988, government statistics noted 6,552 rallies involving 1.7 million people. There were 2.2 million people who had participated in 6,791 demonstrations in 1989.

Listening to North Korean radio stations remained illegal in 1990 if it were judged to be for the purpose of “benefiting the anti-state organization” (North Korea). Similarly, books or other literature considered subversive, procommunist, or pro-North Korean were illegal; authors, publishers, printers, and distributors of such material were subject to arrest.

As of 1990, the organizational structure of the NSP was considered classified by Seoul, although earlier organizational information was public knowledge. Despite the social and political changes that came with the Sixth Republic, the NSP apparently still considered the support and maintenance of the president in power to be one of its most important roles. In April 1990, for example, ruling Democratic Liberal Party (DLP) coleader Kim Young Sam complained that he and members of his faction within the DLP had been subjected to “intelligence maneuvering in politics” that

included wiretapping, surveillance, and financial investigations.

Nevertheless, the NSP's domestic powers were indeed curtailed under the Sixth Republic. Prior to the change, the NSP had free access to all government offices and files. The NSP, Defense Security Command, Office of the Prosecutor General, Korean National Police, and the Ministry of Justice had stationed their agents in the National Assembly to collect information on the activities of politicians. In May 1988, however, overt NSP agents, along with agents of other intelligence agencies, were withdrawn from the National Assembly building. The NSP's budget was not made public nor apparently was it made available in any useful manner to the National Assembly in closed sessions. In July 1989, pressured by opposition parties and public opinion, the NSP was subjected to inspection and audit by the National Assembly for the first time in 18 years. The NSP removed its agents from the chambers of the Seoul Criminal Court and the Supreme Court in 1988.

As of 1990, however, the NSP remained deeply involved in domestic politics and was not prepared to relinquish the power to prevent radical South Korean ideas—much less North Korean ideas—from circulating in South Korean society. Despite an agreement in September 1989 by the chief policymakers of the ruling and opposition parties to strip the NSP of its power to investigate pro-North Korean activity (a crime under the National Security Act), the NSP continued enforcing this aspect of the law rather than limiting itself to countering internal and external attempts to overthrow the government. The NSP continued to pick up radical student and dissident leaders for questioning without explanation.

In another move to limit the potential for the NSP to engage in “intelligence politics,” the NSP Information Coordination Committee was disbanded because of its history of unduly influencing other investigating authorities, such as the Office of the Prosecutor General. In addition, the NSP, responding to widespread criticism of its alleged human rights violations, set up

a “watchdog” office to supervise its domestic investigations and to prevent agents from abusing their powers while interrogating suspects.

Aside from its controversial internal security mission, the NSP also was known for its foreign intelligence gathering and analysis and for its investigation of offenses involving external subversion and military secrets. The National Unification Board and the NSP (and the KCIA before it) were the primary sources of government analysis and policy direction for South Korea's reunification strategy and contacts with North Korea. The intelligence service's reputation in pursuing counterespionage cases also was excellent.

The NSP monitored visitors, particularly from communist and East European countries, to prevent industrial and military espionage. Following the diplomatic successes of the late 1980s—the establishment of diplomatic relations with the Soviet Union and the countries of Eastern Europe and the increased informal contacts with China, Mongolia, and Vietnam—this mission grew in importance. The security watch list contained 162 out of 3,808 visitors from communist nations in 1988 and 226 out of 6,444 visitors in 1989.

In 1995, by relocating to a new intelligence building equipped with up-to-date facilities in Naegok-dong (southern Seoul) from its 34-year-old site in Mt. Nam in downtown Seoul and Imun-dong (eastern Seoul), the NSP laid the cornerstone to become a 21st century, advanced intelligence agency. With the inauguration of the People's Government on 22 January 1999, the agency was renamed the National Intelligence Service (NIS). The former Minister of Defense Chun Yong-taek took office as the 23rd Director General of the National Intelligence Service on 26 May 1999. He had served as National Assemblyman, Party member of the Government of the People, Minister of Defense, and Lieutenant General in the armed forces reserve.

National Intelligence Service missions and functions include:

- Collection, coordination, and distribution of information on the nation's strategy and security.
- Investigation of crimes affecting national security, including crimes that violate the Military Secrecy Protection Law and the National Security Law that prohibit the incitement of civil war, foreign troubles, and insurrection.
- Investigation of crimes related to the missions of NIS staff.
- Maintenance of documents, materials, and facilities related to the nation's classified information.
- Planning and coordination of information and classified information.

Government and Private-Sector Efforts To Steal US Technological Secrets

In the mid-1990s, South Korean media began reporting that, over the past two years, the Republic of Korea (ROK) Government and South Korean companies were engaging in systematic efforts to obtain foreign proprietary technology through indirect methods. Faced with a decline in the competitiveness of its products, the high cost of buying foreign technology, and the difficulty of developing new technology through its own resources, South Korea reportedly contrived a host of oblique means to access the technological secrets of advanced countries.

According to these ROK press reports, these techniques ranged from the use of academic exchange programs to the use of the country's intelligence service for industrial espionage. Several of these technical acquisition programs reportedly targeted US citizens through databases and through recruitment programs focused on expatriate Koreans. Many such initiatives reportedly were designed and managed by the ROK Government itself. The press described South Korea's methods to obtain foreign technology, particularly from US companies. Of note, the press reported that ROK firms were losing interest in

Japan, traditionally South Korea's main technology source, because the Japanese demanded high royalties for technology transfers.

The most-wanted technologies sought from the United States by South Korean companies and government research institutes were aerospace, automobiles, bioengineering, computers, communications, electronics, environmental, machinery and metals, medical equipment, nuclear power, and semiconductors. Within these areas, the South Koreans frequently targeted electronics, data communications and processing, and semiconductor technology—South Korea's major high-tech export fields. These data were based on reported cases of attempted technology transfer and press reports of the targeted fields. Within the frequently targeted group, the highest priorities included high-speed CD-ROM, ultra-high-resolution monitor design, traffic-control systems, flash memory, digital signal processors, application-specific integrated circuits of all types, cable television converters, digital communications, image-data processing, asynchronous transmission-mode technology, fiber optics, and audio-video compression technology.²

South Korea's eagerness to assimilate foreign technology without paying royalties is reflected in the variety of indirect transfer techniques:

- Academic cooperation:
 - *Centers of excellence.* Setting up "centers" staffed by leading foreign institutes provides ROK researchers with opportunities to "come into contact" with high-level scientists and advanced equipment.³
 - *Academic exchanges.* Under this strategy, the South Korean Government sends ROK researchers abroad to acquire advanced technology through their studies.⁴
 - *Technical links to foreign universities.* Large South Korean manufacturers form "international industrial-academic cooperative associations" with foreign universities to do "joint research" in advanced technology.⁵

-
- International cooperation:
 - *International research projects.* Because the initial focus of this research is noncommercial, foreign companies reportedly are more willing to share their technology than they would through conventional channels.⁶
 - *International forums and foundations.* The South Korean Government has sanctioned the establishment of “S&T forums” to act as a corridor between the ROK’s commercial science and technology (S&T) establishment or state-subsidized “foundations” and US high-tech companies to facilitate the transfer of US technology.⁷
 - Cooperation between South Korea and foreign companies:
 - *Strategic cooperation.* This process involves identifying gaps in indigenous technology, finding a foreign company that has the technology, and engaging the latter in some kind of cooperative relationship that results in the transfer of the technology to South Korea.⁸
 - *Joint “research” and development.* When South Korean technicians obtain foreign technology through the development process as part of a transfer agreement, which the South Korean press described as “joint development”.⁹
 - Obtaining foreign patents:
 - *Bargain basement patents.* A large number of ROK firms and research institutes have been obtaining needed technology through cheap patents acquired in Russia.¹⁰
 - *Buyouts of foreign firms.* ROK press reports reveal that buyouts of high-tech foreign companies are another popular way to obtain patented technology.¹¹
 - Employing foreign talent:
 - *Hiring overseas specialists.* Hiring foreign experts is another favored, low-cost means used by South Korea to transfer technology indirectly; it is recommended by government experts, facilitated by official and semiofficial ROK organizations, and widely practiced in ROK industries.¹²
 - *“Brain pools.”* South Korea’s government and industry also operate systems to identify potential recruits who are in a position to transfer high-level technology and, because of their ethnicity, are predisposed to accept offers to “contribute” their knowledge to South Korea.¹³
 - Direct overseas involvement:
 - *Overseas technical training.* On-site training at overseas companies allows South Korea to obtain technology at a fraction of its market cost.¹⁴
 - *Establishing overseas subsidiaries.* Judging by press reports, South Korean firms have also discovered that overseas branches provide another shortcut to technology transfer.¹⁵
 - *Overseas “research centers.”* In addition to obtaining technology through overseas subsidiaries, South Korean companies acquire foreign technology by establishing “research” facilities abroad and staffing them with host-country scientists who transfer knowledge of technological processes to their employers, according to ROK press reports.¹⁶
 - Collection networks:
 - *International trade organizations.* The Korea Trade Promotion Corporation—an ROK Government-run organization that is officially chartered to facilitate the export of South Korean products and that has 81 overseas trade offices—also promotes technology transfer.¹⁷
 - *Employees as intelligence collectors.* ROK firms also have discovered that ordinary employees can yield a wealth of information on competitors’ technologies and plans. Although this does not necessarily lead to technology transfer, it does allow corporations to get a pulse on worldwide research and development (R&D) activities and to use this information in its own policies.¹⁸

-
- *Ethnic and personal relationships.* Substantial media documentation exists on South Korea's interest in exploiting the ethnicity of overseas Koreans to obtain commercial and technological information.¹⁹
 - *Foreign databases.* ROK Government institutes have also helped facilitate the transfer of technology by providing South Korean companies access to foreign databases with industrial, scientific, and technological data from foreign and domestic sources.²⁰

- Commercial espionage:
 - *National intelligence service.* South Korea's NSP is also involved in the indirect transfer of foreign technology.²¹
 - *Corporate spying.* In addition to government-sanctioned efforts to collect technological information, Seoul media report widespread industrial espionage by South Korean companies against each other to obtain a competitor's proprietary technology.²²

South Korea's Informal Technology Acquisitions

Despite its efforts, South Korea continued to suffer economic difficulties during the mid-1990s. As part of its uphill struggle to break out of its economic doldrums, South Korea increased its efforts to obtain foreign proprietary technology, according to Seoul media reports. Mechanisms through which enhanced collection activity was reported included "joint research," recruitment of foreign nationals, outposts located in high-tech regions abroad, expatriate scientists, and the National Intelligence Service's apparatus. In addition, the South Korean Government reportedly formed a new committee to systematize foreign technology collection and expand the number of overseas collectors.

The South Korean press reported an intensification of the country's efforts to obtain foreign technology through informal channels that was attributed, in part, to strains in the ROK economy. While

earlier collection efforts were motivated by what the media described as a shortage of "wellspring technology," other factors such as "snowballing" royalty payments²³ and the then-financial crisis were cited as causes for renewed emphasis on this practice.

South Korea's national laboratories were tasked by the government to "help domestic industry overcome the economic crisis" by rendering "practical" support for new product development and by "Internationalizing their research activities."²⁴ Examples of the latter included the Korea Institute of Science and Technology's (part of the Ministry of Science and Technology—MOST) program to "conduct personnel exchanges, information interchange, and joint research with 57 institutions in 19 countries." The Korean Institute of Machinery and Metals' (another MOST affiliate) planned to set up joint R&D centers at Stanford University and MIT to "acquire leading future technologies." South Korea also sought US Government backing to expand these "cooperative exchanges" across a wide range of "state-of-the-art technologies."²⁵

European countries also were increasingly targeted as sources of new technology. South Korean science officers stationed at 10 ROK Government-funded research centers in Europe and Russia met in Paris to discuss ways to boost their research activity, described by one officer as the "systematic gathering of information on [host country] research institutes, technologies, and personnel."²⁶

Direct exploitation of overseas scientists by ROK Government institutions was being stepped up by expanding the "brainpool" project according to an Internet posting by the Korea-American Scientists and Engineers Association (KSEA), read on 2 February 1998 through a mirror site in Seoul. Administered by MOST and executed through eight national chapters (United States, Canada, United Kingdom, France, Germany, Japan, China, and Australia) of the Seoul-based General Federation of Korean Science and Technology Organizations, the project offers salaries and expenses to "outstanding scientists and engineers

from overseas” to share their knowledge in “all fields of science and technology” with their counterparts at ROK national and corporate laboratories. In previous years, the notices capped the number of positions to a few dozen, whereas in 1998, the solicitation appeared to be open-ended.

ROK companies likewise were increasingly eager to tap the expertise of foreign scientists. The major groups’ electronic subsidiaries “launched an aggressive ‘head hunting’ operations” overseas aimed at scientists and engineers in electronics and information science.²⁷ Samsung Electronics reportedly held briefing sessions and recruitment exhibitions “at major universities and research institutes in the United States and Europe.” LG Electronics, Hyundai Electronics (through the use of an Internet-based “manpower management program”) and Daewoo Electronics matched Samsung’s efforts. It was noted that Daewoo, in particular, was “securing competent employees overseas by using Korean students studying abroad on company scholarships, its overseas branches, and its own research institutes established in the United States, Japan, and Europe as an information network. The overseas recruitment of scientific talent was being pursued at the group level and focused not only on established scientists but also on new graduates of prestigious US technical universities.”²⁸

Besides these company-led efforts, South Koreans were establishing independent “consulting firms” overseas whose function is to “scout out technical manpower for Korean companies” and broker the transfer of “core technologies” to ROK producers.²⁹ One such company reportedly was established in Moscow by “specialists engaged in technology transfers from Russia on behalf of large Korean businesses.” Another Korean consulting firm opened offices in Moscow and Los Angeles to “recruit high-tech personnel in data communications.” A personnel officer from an ROK company stated to the effect that fees of \$100,000 are not considered excessive for the services of a top foreign scientist and speculated that “hiring advanced specialists from foreign countries” would increase.³⁰

The United States’ Silicon Valley is a favorite venue for informal technology transfers through ROK Government-backed outposts for marketing and “information exchange.” According to a Ministry of Information and Communications (MIC) press release of 17 November 1997, South Korea was funding the creation of “incubators” in Silicon Valley designed both to promote the sale of ROK software products and conduct “technology exchange activities.”

Korea Telecom, a public corporation, was to create a capital fund with ROK communications equipment manufacturers to support Silicon Valley-based American venture enterprises in advanced data communications.³¹ The Korea Advanced Institute of Science and Technology (a MOST subsidiary) funded the establishment of a semiconductor equipment-manufacturing firm in Silicon Valley, which is run by expatriate Koreans. The firm reportedly is designed to allow ROK graduate students “to acquire technology at the same time they earn dollars” by performing research with world-class engineers.³²

Coordinating S&T collection efforts and integrating collection targets with the needs of ROK manufacturers—long a “bottleneck” in South Korea’s informal technology-transfer programs—entered a “new dimension” as a result of programs undertaken by MOST’s Science and Technology Policy Institute (STEPI).³³ According to a report released by STEPI on 9 December 1998 cited by the Korean press, the separate collection programs run by the Ministries of Foreign Affairs, Trade and Industry, National Defense, and Science are to be brought together under a “Science and Technology Foreign Cooperation Committee” meant to systematize collection strategy, integrate local operations, and avoid duplication of effort. The committee reportedly would be divided into groups of specialists by geographical region who would interact with a council composed of working-level personnel from organizations such as the Korea Trade Promotion Agency (KOTRA) and STEPI on the one hand, and national labs, universities, and ROK companies on the other.

Reportedly formed to counter the “increasing reluctance of advanced countries to transfer their science and technology,” the program entails establishing local “Korea Centers” to collect foreign S&T information and to set up overseas branches of government bodies, national labs, and companies “to provide information on foreign S&T.”³⁴ Moreover, to “strengthen overseas S&T collection” and build an information system that would link ROK organizations to overseas sources of technology, STEPI was to create an “Overseas Science and Technology Information Center” that integrates the S&T information collected by “overseas Korean scientists and engineers associations, Korean diplomatic and consular offices in foreign countries, large Korean trading companies, and the overseas offices of national labs.”

In this connection, the Korean-US Science Cooperation Center, an ROK Government-funded S&T collection facility and host to the KSEA, is now five years old. Items posted on its Internet Web site included a comprehensive directory (with hotlinks to major US Government technology centers, national laboratories, and professional scientific organizations), along with an invitation for proposals to create new programs designed to promote S&T cooperation and to help “Korean and American scientists develop and maintain permanent S&T networks.” KSEA, for its part, promoted on its Web site STEPI’s “Creative Research Initiative Program” that sought to fill some 45 South Korean research associate positions with foreign or expatriate scientists in 1998.

In 1997, the president-elect, Kim Dae-jung, drafted reforms for the NSP that entailed an “intensive buildup of economic information-collecting capabilities” against overseas targets.³⁵

Cooperation Centers To Acquire Technologies

In March 2001, South Korea’s Small and Medium Business Administration began to screen applicants for admission to a newly established Korea Venture

Center (KVC) in Fairfax County, Virginia. Of the 35 South Korean venture companies that applied for entry into the US-based high-tech “incubator,” 10 were to be selected to receive support at the Center. This support reportedly included subsidized rent and guidance in finding local firms for technical cooperation.³⁶

The KVC is the first South Korean center in the eastern United States. Its formation was announced by South Korea’s Ministry of Commerce, Industry, and Energy (MOCIE) as part of that country’s effort to promote “strategic cooperation” with US firms in high-tech corridors of the United States.³⁷ At its formal opening in late November 2000, KVC Director U Chong-sik reiterated that the Center’s goal is to assist Korean companies in arranging joint R&D with foreign institutions.³⁸

The KVC was South Korea’s third information technology (IT) incubator in the United States; the other two being the Overseas Software Support Center (KSI) and the Information and Communications Venture Support Center (I-park) in Silicon Valley, both under the MIC. The 14 companies at KSI were to relocate to I-park at the end of 2001, in connection with a merger of the two facilities that was driven by the need to directly support their clients’ interaction with local high-tech firms.³⁹

I-park is involved in technology transfer by “facilitating strategic cooperation with local US companies,” a phrase used in the Korean press to describe programs aimed at acquiring foreign technology.⁴⁰ I-park serves as a base of operations for a network of ethnic Korean IT specialists in Silicon Valley, which suggests that the South Korean venture companies are encouraged to pursue technical ties to émigré IT companies already operating in the valley.⁴¹

I-park’s role as a technology-transfer installation was stated on its Web site, which listed facilitating technology exchanges as a main function. The site acknowledged support from the Institute of Information Technology Assessment (IITA),

whose primary Web site identified technology transfer as one of its main projects. The IITA was founded in 1992 as an affiliate of the Electronics and Telecommunications Research Institute (ETRI), now part of MIC, South Korea's state-run telecommunications research facility chartered to disseminate innovative technology to Korean manufacturers.

The link between tech transfer and the KVC/I-park operations is further underscored by IITA's association since October 1999 with Seoul's IT Technology Transfer Center, also referred to as a cyber technomart, which is designed to facilitate the early acquisition of state-of-the-art technology and its commercialization by South Korean manufacturers, according to the Center's Web site. I-park itself is referred to in some Seoul press reports⁴² and IITA's "History" pages as the Overseas IT technology cooperation center.

In a related event, MOCIE planned to establish a similar Japan IT venture center in Tokyo at the end of February 2001 to support South Korean venture firms' strategic cooperation with high-tech Japanese telecommunications companies. The new center, based on a Korean-Japan IT cooperation initiative signed in September 2000, reportedly would maintain contact with the KVC in Fairfax County.⁴³

Science Ministry Continues Foreign Recruitment Drive

The South Korean Government is continuing its efforts to recruit ethnic Korean scientists abroad to support state and corporate-defined research programs, as evidenced by a Science Ministry posting that called for a transnational "brainpool." The pragmatic nature of these efforts was brought out in the posting, which emphasized the importance of making concrete contributions to the country's S&T agenda.

According to a notice posted in April 2001 on the South Korean Science Ministry's Web site, the ministry, in conjunction with liaison organizations,

renewed its sponsorship of a "brainpool" project to recruit foreign technical specialists willing to share their accumulated expertise with Seoul. The notice read in part:

The General Federation of Korean S&T Organizations, in accordance with the government's (Ministry of Science and Technology) plan to recruit and make use of high-level overseas scientists (brainpool), is seeking world-class superior overseas scientists and engineers willing to contribute to raising our country's international competitiveness for on-site work at colleges, companies, and South Korean R&D facilities. We hope for your wide participation.

The notice invited overseas scientists with recognized skills in areas "targeted for national strategic development" to apply. Some 30 different fields were listed, ranging from basic science to applied technology. Employment reportedly involved working with an existing R&D team or one formed around the scientist's area of expertise. Lecturing at seminars and before "scholarly associations" is also an option. Appointments ranged from three months to two years.

The ministry advised that applicants should be "overseas Korean or foreign scientists and engineers" with more than five years postdoctoral experience in a foreign country. However, exceptions would be made for those who demonstrated outstanding research ability or who "possess know-how." Scientists who have worked five years in a foreign firm's research lab need not hold a doctorate.

Technology-Transfer Facility in San Diego

A quasi-official ROK industrial organization was to work with South Korean biotechnology companies to establish a technology-transfer facility in San Diego. The South Korean Government would subsidize the new center, which would facilitate "networking" with local researchers.

The Federation of Korean Industries (FKI), which is South Korea's largest industrial organization and serves as an intermediary between ROK companies and government policy makers, proposed in late October 2001 that a "Korea Bio Valley" be set up near San Diego to serve as a focal point for entry of ROK products into the US market and to facilitate acquisition of US biotechnology. FKI's plan called for joint participation by large ROK companies, pharmaceutical makers, and biotech startups in establishing this "bridgehead" into the US "hub" of the life sciences industry.⁴⁴

Bio Valley would support 10 to 15 ROK companies in the Carlsbad district of San Diego. The ROK Government reportedly would buy buildings and other infrastructure and lease them to Korean companies or make them available at no cost. Ten billion won of the 15-billion won budget would be covered by public subscriptions with the remainder provided as a government subsidy.⁴⁵ FKI would work with the Korea Bioventure Association, South Korea's major biotech industrial group, to complete the complex by 2001. However, the plans to establish the "Korea Bio-Park" have been hit by delays over budget problems. The Ministry of Commerce, Industry and Energy has yet to set aside a budget for the project. Also, Korean companies and bio-venture firms, which are to help finance the project, are suffering financial difficulties. The plan is currently in limbo.

Bio Valley is part of a larger FKI proposal titled "A Plan for Developing the Biotech Industry (October 2001)" aimed at raising the technology level of domestic biotech firms. According to a copy of the plan posted to FKI's Web site, the main purpose of the US complex is "to grasp in real time the latest advances in biotechnology and trends in the biotech industry." The plan states that Korea's "R&D capability will be improved by making use of top-notch overseas research personnel and networking with them." A secondary goal is noted as promoting "with a minimum investment, the introduction of ROK biotech products into the United States and adjacent countries."

Seoul's move to establish a high-tech "liaison center" in the heartland of the US biotech industry parallels its successful efforts noted above to comb Silicon Valley for information technology, a field where South Korea now enjoys some commanding leads. An example of this approach is the so-called "Information and Communications Venture Support Center" in San Jose, identified recently in South Korean press reports as an information technology-transfer facility sponsored by the ROK Government.

Endnotes

- ¹ This article is based on Library of Congress information and articles written by the National Counterintelligence Center and its successor, the National Counterintelligence Executive.
- ² *Hanguk Kyongje Sinmun*, *Maeil Kyongje Sinmun*, various dates in 1994 and 1995.
- ³ *Maeil Kyongje Sinmun*, 29 January 1995.
- ⁴ *Korea Herald*, 14 January 1995.
- ⁵ *Hanguk Kyongje Sinmun*, 23 January 1995.
- ⁶ *Hanguk Kyongje Sinmun*, 25 June 1994.
- ⁷ *Maeil Kyongje Sinmun*, 25 May 1994.
- ⁸ *Maeil Kyongje Sinmun*, 24 January 1994.
- ⁹ *Maeil Kyongje Sinmun*, 10 January 1995.
- ¹⁰ *Hanguk Kyongje Sinmun*, 31 January 1994.
- ¹¹ *Maeil Kyongje Sinmun*, 3 February 1995.
- ¹² *Hanguk Kyongje Sinmun*, 13 July 1994.
- ¹³ *Maeil Kyongje Sinmun*, 19 May 1993.
- ¹⁴ *Hanguk Kyongje Sinmun*, 25 March 1993.
- ¹⁵ *Hanguk Kyongje Sinmun*, 17 May 1993.
- ¹⁶ *Hanguk Kyongje Sinmun*, 16 January 1995.
- ¹⁷ *Hanguk Kyongje Sinmun*, 25 July 1994.
- ¹⁸ *Hanguk Kyongje Sinmun*, 25 June 1994.
- ¹⁹ *Hanguk Kyongje Sinmun*, 14 February 1994.
- ²⁰ *Chonja Sinmun*, 19 March 1994.
- ²¹ *Changang Ilbo*, 6 May 1993.
- ²² *Hangyore Sinmun*, 29 July 1993.
- ²³ Reported in the 5 August 1997 and 30 September 1997 issues of *Chonja Sinmun*.
- ²⁴ *Chonja Sinmun*, 10 January 1998.
- ²⁵ *Yonhap*, 14 January 1998.
- ²⁶ *Chonja Sinmun*, 9 October 1997.
- ²⁷ *Chonja Sinmun*, 30 September 1997.
- ²⁸ *Hanguk Kyongje*, 27 September 1997.
- ²⁹ *Maeil Kyongje Sinmun*, 9 September 1997.
- ³⁰ *Maeil Kyongje Sinmun*, 5 December 1997.
- ³¹ *Maeil Kyongje Sinmun*, 14 November 1997.
- ³² *Maeil Kyongje Sinmun*, 14 January 1998.
- ³³ *Chonja Sinmun*, 10 December 1997.
- ³⁴ Ibid.
- ³⁵ *Yonhap*, 26 and 29 December 1997.
- ³⁶ *Chonja Sinmun*, 8 February 2001.
- ³⁷ *Chonja Sinmun*, 20 October 2000.
- ³⁸ *Hanguk Kyongje Sinmun*, 21 November 2000.
- ³⁹ *Chonja Sinmun*, 21 December 2000.
- ⁴⁰ *Maeil Kyongje Sinmun*, 29 May 2000.
- ⁴¹ *Hanguk Ilbo*, 3 September 2000.
- ⁴² See *Hanguk Kyongje Sinmun*, 7 October 2000.
- ⁴³ *Naewoe Kyongje Sinmun*, 7 December 2000.
- ⁴⁴ *Chonja Sinmun*, 31 October 2000.
- ⁴⁵ *Hanguk Kyongje Sinmun*, 31 October 2000.

CHAPTER 4

INTRODUCTION

On 18 March 1999, the President requested the President's Foreign Intelligence Advisory Board (PFIAB), chaired by former Senator Warren Rudman, to review the security threat at DOE's nuclear weapons laboratories and the measures that have been taken to address that threat. On 15 June 1999, the PFIAB presented its report, *Science at Its Best—Security at Its Worst* (the "Rudman report"), to the President. The report found that DOE "is a dysfunctional bureaucracy that has proven it is incapable of reforming itself." The report stated that the "nuclear weapons and research functions of DOE need more autonomy, a clearer mission, a streamlined bureaucracy, and increased accountability."

Following its extensive 1999 review of DOE security and counterintelligence (CI) problems, the House Intelligence Committee continued its oversight over DOE's CI and intelligence programs. The Committee closely monitored DOE's implementation of Presidential Decision Directive-61 (PDD-61)—the DOE Counterintelligence Implementation Plan and the National Defense Authorization Act of Fiscal Year 2000—to ensure that DOE followed through on these and other long-overdue reforms. The Committee was disappointed that, in DOE's initial CI inspections of the major weapons laboratories, only one lab—Lawrence Livermore National Laboratory—received a satisfactory rating. The Committee was also concerned that neither the DOE Director of CI, the DCI, nor the FBI Director could certify to Congress that DOE's foreign visitors program complied with applicable DOE directives and PDD and similar requirements and did not pose an undue risk to US national security.

Congressional concern over security at the nuclear weapons laboratories increased again in June 2000 when several computer hard drives containing nuclear weapons information were lost at Los Alamos. The hard drives were later found

behind a photocopier close to the vault where the drives were stored. The FBI, which had been investigating the disappearance of the hard drives, believed that one or possibly more scientists took the drives from the vault in April and misplaced them. Fearful of possible punishment for a security lapse, the scientist or scientists engaged in the coverup—put the drives behind the copier.

During the previous seven years, new CI mechanisms to address economic and industrial espionage were created and procedures implemented to improve coordination among intelligence, CI, and law enforcement agencies. It was felt that these measures had considerably strengthened the US Government's ability to counter the foreign intelligence threat. However, there was a difference of opinion.

On 8 March 2000, during a closed hearing before the Senate Select Committee on Intelligence (SSCI), DCI George Tenet, FBI Director Louis Freeh, and Deputy Secretary of Defense John Hamre unveiled a draft proposal entitled "Counterintelligence for the 21st Century." This plan, generally referred to as "CI 21," resulted from an extensive review assessing existing CI structures and capabilities to address emerging, as well as traditional, CI issues. The drafters of the CI 21 plan found current US CI capabilities to be "piecemeal and parochial," and recommended adoption of a new CI philosophy—described as more policy-driven, prioritized, and flexible, with a strategic, national-level focus—as well as a restructured national CI system. CI 21 proposed significant changes in the way the US Government approaches and organizes itself to meet the threat of foreign espionage and intelligence gathering.

Congress noted that the FBI's National Infrastructure Protection Center (NIPC)—charged with detecting, preventing, and responding to cyber and physical attacks on US critical

infrastructures—and the new Office of National Counterintelligence Executive (NCIX) had similarities in mission and interagency focus. This prompted Congress to suggest that both these offices be co-located at one site. They directed a joint written assessment be done by the NCIX Executive, the DCI, and the FBI Director and provide to the intelligence oversight committees. This assessment, of the desirability and feasibility (including a budgetary assessment) of colocating the NIPC and NCIX at one site, separate and apart from CIA, FBI, and Department of Defense facilities, was due by sometime in late 2002.

The Fiscal Year 2001 Intelligence Authorization Bill had provisions to establish criminal penalties for the unauthorized disclosure of properly classified information. Previous legislation established penalties only for disclosure of specific types of classified material—codes and cryptographic devices and information related to nuclear programs. After some debate about the provision, President William Clinton vetoed the bill on 4 November 2000. Another version of the FY2001 authorization bill without the disclosure provision was enacted on 27 December 2000. Proponents

of the provision tried again after President George W. Bush came into office, but nonsupport from the White House again killed the provision.

Leaks continue to plague the government and the Intelligence Community. This was quite evident by information being made available to the media by Congress relating to the US war against terrorism following the 11 September 2001 destruction of the World Trade Center Towers in New York and part of the Pentagon by terrorists using hijacked US airlines. President Bush ordered that only a few selected members of Congress were to be briefed. Still, the media obtained classified information and published it.

The Rudman Report

(Editor's Note: The following is an edited summary of the Rudman Report.)

On 18 March 1999, President William J. Clinton requested that the President's Foreign Intelligence Advisory Board (PFIAB) undertake an inquiry and issue a report on "the security threat at the Department of Energy's (DOE) weapons labs and the adequacy of the measures that have been taken to address it."

Specifically, the President asked the PFIAB to "address the nature of the present counterintelligence security threat, the way in which it has evolved over the last two decades and the steps we have taken to counter it, as well as to recommend any additional steps that may be needed." He also asked the PFIAB "to deliver its completed report to the Congress, and, to the fullest extent possible consistent with our national security, release an unclassified version to the public."

This report, including an appendix of supporting documents, is unclassified. A large volume of classified material, which was also reviewed and distilled for this report, has been relegated to a second appendix that is available only to authorized recipients. This report examines:

- The 20-year history of security and counterintelligence issues at the DOE national laboratories, with an emphasis on the five labs that focus on weapons-related research.
- The inherent tension between security concerns and scientific freedom at the labs and its effect on the institutional culture and efficacy of DOE.
- The growth and evolution of the foreign intelligence threat to the national labs, particularly in connection with the Foreign Visitor's Program.
- The implementation and effectiveness of Presidential Decision Directive No. 61, the

reforms instituted by Secretary of Energy Bill Richardson, and other related initiatives.

- Additional measures that should be taken to improve security and counterintelligence at the labs.

Foreword From the Special Investigative Panel

For the past two decades, DOE has embodied science at its best and security of secrets at its worst.

Within DOE are a number of the crown jewels of the world's government-sponsored scientific research and development organizations. With its record as the incubator for the work of many talented scientists and engineers—including many Nobel prize winners—DOE has provided the nation with far-reaching advantages. Its discoveries not only helped the United States to prevail in the Cold War, but they undoubtedly will also continue to provide both technological benefits and inspiration for the progress of generations to come. The vitality of its national laboratories is derived to a great extent from their ability to attract talent from the widest possible pool, and they should continue to capitalize on the expertise of immigrant scientists and engineers. However, we believe that the dysfunctional structure at the heart of DOE has too often resulted in the mismanagement of security in weapons-related activities and a lack of emphasis on counterintelligence.

DOE was created in 1977 and heralded as the centerpiece of the federal solution to the energy crisis that had stunned the American economy. A vital part of this new initiative was the Energy Research and Development Administration (ERDA), the legacy agency of the Atomic Energy Commission (AEC) and inheritor of the national programs to develop safe and reliable nuclear weapons. The concept, at least, was straightforward: take the diverse and dispersed energy research centers of the nation, bring them under an umbrella organization with other energy-related enterprises, and spark their scientific progress through closer contacts and centralized management.

However, the brilliant scientific breakthroughs at the nuclear weapons laboratories came with a very troubling record of security administration. For example:

- Classified documents detailing the designs of the most advanced nuclear weapons were found at the Los Alamos laboratory on library shelves accessible to the public.
- Employees and researchers were receiving little, if any, training or instruction regarding espionage threats.
- Multiple chains of command and standards of performance negated accountability, resulting in pervasive inefficiency, confusion, and mistrust.
- Competition among laboratories for contracts and among researchers for talent, resources, and support distracted management from security issues.
- Sloppy accounting bedeviled fiscal management.
- Inexact tracking of the quantities and flows of nuclear materials was a persistent worry.
- Geographic decentralization fractured policy implementation, and changes in leadership regularly depleted the small reservoirs of institutional memory.

Permeating all of these issues was a prevailing cultural attitude among some in the DOE scientific community that regarded the protection of nuclear know-how with either fatalism or naivete.

In response to these problems, DOE has been the subject of a nearly unbroken history of dire warnings and attempted but aborted reforms. A cursory review of the open-source literature on the DOE record of management presents an abysmal picture. Second only to its world-class intellectual feats has been its ability to fend off systemic change. Over the last dozen years, DOE has averaged some kind of major departmental shakeup every two to three years. No President, Energy Secretary, or Congress has been able to stem the recurrence of fundamental problems. All have been thwarted time after time by the intransigence of this institution. The Special Investigative Panel found a large organization saturated with cynicism, an arrogant disregard for authority, and a staggering

pattern of denial. For instance, even after President Clinton issued Presidential Decision Directive 61 ordering DOE to make fundamental changes in security procedures, compliance by Department bureaucrats was grudging and belated.

Repeatedly over the past few decades, officials at DOE Headquarters and at the weapons labs have been presented with overwhelming evidence that their lackadaisical oversight could lead to an increase in the nuclear threat against the United States. Throughout its history, DOE has been the subject of scores of critical reports from the General Accounting Office (GAO), the Intelligence Community, independent commissions, private management consultants, its Inspector General, and its security experts. It has repeatedly attempted reforms. Yet the DOE's ingrained behavior and values have caused it to continue to falter and fail.

Prospects for Reforms

We believe that Secretary of Energy Richardson, in attempting to deal with many critical security matters facing the Department, is on the right track regarding some, though not all, of his changes. We concur with and encourage many of his recent initiatives, and we are heartened by his aggressive approach and command of the issues. But we believe that he has overstated the case when he asserts, as he did several weeks ago, that "Americans can be reassured: our nation's nuclear secrets are, today, safe and secure."

After a review of more than 700 reports and studies, thousands of pages of classified and unclassified source documents, interviews with scores of senior federal officials, and visits to several of the DOE laboratories at the heart of this inquiry, the Special Investigative Panel has concluded the Department of Energy is incapable of reforming itself—bureaucratically and culturally—in a lasting way, even under an activist Secretary.

The panel has found that DOE and the weapons laboratories have a deeply rooted culture of low regard for and, at times, hostility toward security issues, which has continually frustrated the efforts

of its internal and external critics, notably the GAO and the House Energy and Commerce Committee. Therefore, a reshuffling of offices and lines of accountability may be a necessary step toward meaningful reform, but it almost certainly will not be sufficient.

Even if every aspect of the ongoing structural reforms is fully implemented, the most powerful guarantor of security at the nation's weapons laboratories will not be laws, regulations, or management charts. It will be the attitudes and behavior of the men and women who are responsible for the operation of the labs each day. These attitudes will not change overnight, and they are likely to change only in a different cultural environment—one that values security as a vital and integral part of day-to-day activities and believes it can coexist with great science.

We are convinced that when Secretary Richardson leaves office his successor is not likely to have a comparable appreciation of the gravity of the Department's past problems nor a comparable interest in resolving them. The new secretary will have a new agenda to pursue and may not focus on DOE's previous mismanagement of national secrets. Indeed, the core of the Department's bureaucracy is quite capable of revising Secretary Richardson's reforms and may well be inclined to do so if given the opportunity.

Ultimately, the nature of the institution and the structure of the incentives, under a culture of scientific research, require great attention if they are to be made compatible with the levels of security and the degree of command and control warranted where the research and stewardship of nuclear weaponry is concerned. Yet it must be done.

Solutions

Our panel has concluded that the Department of Energy, when faced with a profound public responsibility, has failed. Therefore, this report suggests two alternative organizational solutions, both of which we believe would substantially insulate the weapons laboratories from many of DOE's historical

problems and, over time, promote the building of a responsible culture. We also offer recommendations for improving various aspects of security and counterintelligence at DOE, such as personnel assurance, cyber security, program management, and interdepartmental cooperation under the Foreign Intelligence Surveillance Act of 1978.

- The weapons research and stockpile management functions should be placed wholly within a new semiautonomous agency within DOE that has a clear mission, streamlined bureaucracy, and drastically simplified lines of authority and accountability. Useful lessons along these lines can be taken from the National Security Agency (NSA) or Defense Advanced Research Projects Agency (DARPA) within the Department of Defense or the National Oceanographic and Atmospheric Administration (NOAA) within the Department of Commerce.
- A wholly independent agency, such as the National Aeronautics and Space Administration (NASA), should be created.

There was substantial debate among the members of the panel regarding the strengths and weaknesses of these two alternatives. In the final analysis, whether to adopt or reject either of the above solutions rests in the hands of the President and the Congress, and we trust that they will give serious deliberation to the merits and shortcomings of the alternatives before enacting major reforms. We all agree, nonetheless, that the labs should never be subordinated to the Department of Defense.

With either proposal it will be important for the weapons labs to maintain effective scientific contact on unclassified scientific research with the other DOE labs and the wider scientific community. To do otherwise would work to the detriment of the nation's scientific progress and security over the long run. This argument draws on history: nations that honor and advance freedom of inquiry have fared better than those who have sought to arbitrarily suppress and control the community of science.

However, we would submit that we do not face an either/or proposition. The past 20 years have

provided a controlled experiment of a sort, the results of which point to institutional models that hold promise. Organizations such as NASA and DARPA have advanced scientific and technological progress while maintaining a respectable record of security. Meanwhile, the Department of Energy, with its decentralized structure, confusing matrix of crosscutting and overlapping management, and shoddy record of accountability, has advanced scientific and technological progress, but at the cost of an abominable record of security with deeply troubling threats to American national security.

Thomas Paine once said that, “government, even in its best state, is but a necessary evil; in its worst state, an intolerable one.” This report finds that DOE’s performance, throughout its history, should have been regarded as intolerable.

We believe the results and implications of this experiment are clear. It is time for the nation’s leaders to act decisively in the defense of America’s national security.

Bottom Line

DOE represents the best of America’s scientific talent and achievement, but it has also been responsible for the worst security record on secrecy that the members of this panel have ever encountered.

With its record as the incubator for the work of many talented scientists and engineers—including many Nobel Prize winners—DOE has provided the nation with far-reaching advantages. DOE’s discoveries not only helped the United States to prevail in the Cold War, they will also undoubtedly provide both technological benefits and inspiration for the progress of generations to come. Its vibrancy is derived to a great extent from its ability to attract talent from the widest possible pool, and it should continue to capitalize on the expertise of immigrant scientists and engineers. However, the Department has devoted far too little time, attention, and resources to the prosaic but grave responsibilities of security and counterintelligence in managing its weapons and other national security programs.

Findings

The preponderance of evidence accumulated by the Special Investigative Panel, spanning the past 25 years, has compelled the members to reach many definite conclusions—some very disturbing—about the security and well being of the nation’s weapons laboratories.

As the repository of America’s most advanced know-how in nuclear and nuclear-related armaments and the home of some of America’s finest scientific minds, these labs have been and will continue to be a major target of foreign intelligence services, friendly as well as hostile. Two landmark events, the end of the Cold War and the overwhelming victory of the United States and its allies in the Persian Gulf war, markedly altered the security equations and the outlook of nations throughout the world. Friends and foes of the United States intensified their efforts to close the technological gap between their forces and those of America, and some redoubled their efforts in the race for weapons of mass destruction. Under the restraints imposed by the Comprehensive Test Ban Treaty, powerful computers have replaced detonations as the best available means of testing the viability and performance capabilities of new nuclear weapons. Research done by US weapons laboratories with high performance computers stands particularly high on the espionage hit list of other nations, many of which have used increasingly more sophisticated and diverse means to obtain US research necessary to join the nuclear club.

Reports, studies, and formal inquiries written over the past 25 years—by executive branch agencies, Congress, independent panels, and DOE have identified a multitude of chronic security and counterintelligence problems at all of the weapons labs. These reviews produced scores of stern, almost pleading entreaties for change. Critical security flaws in management and planning, personnel assurance, some physical security areas, control of nuclear materials, protection of documents and computerized information, and

counterintelligence have been continuously cited for immediate attention and resolution.

The open-source information on the weapons laboratories overwhelmingly supports a troubling conclusion: for decades their security and counterintelligence operations have been seriously hobbled and relegated to low-priority status. The candid, closed-door testimony of current and former federal officials, as well as the content of voluminous classified materials received by this panel in recent weeks, reinforce this conclusion. When it comes to a genuine understanding of and appreciation for the value of security and counterintelligence programs, especially in the context of America's nuclear arsenal and secrets, the DOE and its weapons labs have been Pollyannaish. The predominant attitude toward security and counterintelligence among many DOE and lab managers has ranged from half-hearted, grudging accommodation to smug disregard. Thus, the panel is convinced that the potential for major leaks and thefts of sensitive information and material has been substantial. Moreover, such security lapses would have occurred in bureaucratic environments that would have allowed them to go undetected with relative ease.

Organizational disarray, managerial neglect, and a culture of arrogance—at both DOE headquarters and the labs—conspired to create an espionage scandal waiting to happen. The physical security efforts of the weapons labs (often called the “guns, guards, and gates”) have had some isolated shortcomings, but on balance they have developed some of the most advanced security technology in the world. However, perpetually weak systems of personnel assurance, information security, and counterintelligence have invited attack by foreign intelligence services. Among the defects, this panel found:

- Inefficient personnel clearance programs, wherein haphazard background investigations could take years to complete and the backlogs numbered in the tens of thousands.
- Loosely controlled and casually monitored programs for thousands of unauthorized foreign scientists and assignees—despite more than a decade of critical reports from the General Accounting Office, the DOE Inspector General, and the Intelligence Community.
- This practice occasionally created bizarre circumstances in which regular lab employees with security clearances were supervised by foreign nationals on temporary assignment.
- Feckless systems for control of classified documents, which periodically resulted in thousands of documents being declared lost.
- Counterintelligence programs with part-time CI officers, who often operated with little experience and minimal budgets and who employed little more than crude “awareness” briefings of foreign threats and perfunctory and sporadic debriefings of scientists traveling to foreign countries.
- A lab security management reporting system that led everywhere except to responsible authority.
- Computer security methods that were naive at best and dangerously irresponsible at worst.

Why were these problems so blatantly and repeatedly ignored? DOE has had a dysfunctional management structure and culture that only occasionally gave proper credence to the need for rigorous security and counterintelligence programs at the weapons labs. For starters, there has been a persisting lack of strong leadership and effective management at DOE.

The nature of the intelligence-gathering methods used by the People's Republic of China (PRC) poses a special challenge to the United States in general and the weapons labs in particular. More sophisticated than some of the blatant methods employed by the former Soviet bloc espionage services, PRC intelligence operatives know their strong suits and play them extremely well. Increasingly more nimble, discreet, and transparent

in their spying methods, the Chinese services have become very proficient in the art of seemingly innocuous elicitation of information. This modus operandi has proved very effective against unwitting and ill-prepared DOE personnel.

Despite widely publicized assertions of wholesale losses of nuclear weapons technology from specific laboratories to particular nations, the factual record in the majority of cases regarding the DOE weapons laboratories supports plausible inferences—but not irrefutable proof—about the source and scope of espionage and the channels through which recipient nations received information. The panel was not charged, nor was it empowered, to conduct a technical assessment regarding the extent to which alleged losses at the national weapons laboratories may have directly advanced the weapons development programs of other nations. However, the panel did find these allegations to be germane to issues regarding the structure and effectiveness of DOE security programs, particularly the counterintelligence functions.

The classified and unclassified evidence available to the panel, while pointing out systemic security vulnerabilities, falls short of being conclusive. The actual damage done to US security interests is, at the least, currently unknown; at worst, it may never be known. Numerous variables are inescapable. Analysis of indigenous technology development in foreign research laboratories is fraught with uncertainty. Moreover, a nation that is a recipient of classified information is not always the sponsor of the espionage by which it was obtained. However, the panel does concur, on balance, with the findings of the recent DCI-sponsored damage assessment. We concur also with the findings of the subsequent independent review, led by Ret. Adm. David Jeremiah, of that damage assessment.

DOE is a dysfunctional bureaucracy that has proven it is incapable of reforming itself. Accountability at DOE has been spread so thinly and erratically that it is now almost impossible to find. The long traditional and effective method of entrenched DOE and lab bureaucrats is to

defeat security reform initiatives by waiting them out. They have been helped in this regard by the frequent changes in leadership at the highest levels of DOE—nine Secretaries of Energy in 22 years. Eventually, DOE’s reform-minded management transitions out, either due to a change in administrations or as a result of the traditional “revolving door” management practices. Then the bureaucracy reverts to old priorities and predilections. Such was the case in December 1990 with the reform recommendations carefully crafted by a special task force commissioned by then-Energy Secretary James D. Watkins (Adm. Ret.). The report skewered DOE for unacceptable “direction, coordination, conduct, and oversight” of safeguards and security. Two years later, the new administration came in, priorities were redefined, and the initiatives all but evaporated. Deputy Secretary Charles Curtis, in late 1996, investigated clear indications of serious security and CI problems and, in response, drew up a list of initiatives. Those initiatives were dropped after he left office.

Reorganization is clearly warranted to resolve the many specific problems with security and counterintelligence in the weapons laboratories and also to address the lack of accountability that has become endemic throughout the entire Department. Layer upon layer of bureaucracy, accumulated over the years, has diffused responsibility to the point where scores claim it, no one has enough to make a difference, and all fight for more. Convoluting, confusing, and often contradictory reporting channels make the relationship between DOE headquarters and the labs, in particular, tense, internecine, and chaotic. In between the headquarters and the laboratories are field offices, which the panel found to be a locus of much confusion. In background briefings of the panel, senior DOE officials often described them as redundant operations that function as a shadow headquarters, often using their political clout and large payrolls to push their own agendas and budget priorities in Congress. Even with the latest DOE restructuring, the weapons labs are reporting far too many DOE masters.

The criteria for the selection of Energy Secretaries have been inconsistent in the past. Regardless of the outcome of ongoing or contemplated reforms, the minimum qualifications for an Energy Secretary should include experience in not only energy and scientific issues, but also national security and intelligence issues. The list of former Secretaries, Deputy Secretaries, and Under Secretaries meeting all of these criteria is very short. Despite having a large proportion (roughly 30 percent) of its budget devoted to functions related to nuclear weapons, DOE has often been led by men and women with little expertise and background in national security. The result has been predictable: security issues have been a low priority, and leaders unfamiliar with these issues have delegated decision-making to lesser-ranking officials who lacked the incentives and authority to address problems with dispatch and forcefulness. For a Department in desperate need of strong leadership on security issues, this has been a disastrous trend. The bar for future nominees at the upper levels of the Department needs to be raised significantly.

DOE cannot be fixed with a single legislative act: management must follow mandate. The research functions of the labs are vital to the nation's long-term interest, and instituting effective gates between weapons and non-weapons research functions will require disinterested scientific expertise, judicious decision-making, and considerable political finesse. Thus, both Congress and the executive branch—whether along the lines suggested by the Special Investigative Panel or others—should be prepared to monitor the progress of the Department's reforms for years to come. This panel has no illusions about the future of security and counterintelligence at DOE. There is little reason to believe future DOE Secretaries will necessarily share the resolve of Secretary Richardson, or even his interest. When the next Secretary of Energy is sworn in, perhaps in the spring of 2001, the DOE and lab bureaucracies will still have advantages that could give them the upper hand: time and proven skills at artful dodging and passive intransigence.

The Foreign Visitors' and Assignments Program has been and should continue to be a valuable contribution to the scientific and technological progress of the nation. Foreign nationals working under the auspices of US weapons labs have achieved remarkable scientific advances and have contributed immensely to a wide array of America's national security interests, including nonproliferation. Some have made contributions so unique that they are all but irreplaceable. The value of these contacts to the nation should not be lost amid the attempt to address deep, well-founded concerns about security lapses. That said, DOE clearly requires measures to ensure that legitimate use of the research laboratories for scientific collaboration is not an open door to foreign espionage agents. Losing national security secrets should never be accepted as an inevitable cost of obtaining scientific knowledge.

In commenting on security issues at DOE, we believe that both Congressional and Executive Branch leaders have resorted to simplification and hyperbole in the past few months. The panel found neither the dramatic damage assessments nor the categorical reassurances of the Department's advocates to be wholly substantiated. We concur with and encourage many of Secretary Richardson's recent initiatives to address the security problems at the Department, and we are heartened by his aggressive approach and command of the issues. He has recognized the organizational dysfunction and cultural vagaries at DOE and has taken strong, positive steps to try to reverse the legacy of more than 20 years of security mismanagement. However, the Board is extremely skeptical that any reform effort, no matter how well-intentioned, well-designed, and effectively applied, will gain more than a toehold at DOE, given its labyrinthine management structure, fractious and arrogant culture, and the fast-approaching reality of another transition in DOE leadership. Thus, we believe that he has overstated the case when he asserts, as he did several weeks ago, that "Americans can be reassured: our nation's nuclear secrets are, today, safe and secure."

Similarly, the evidence indicating widespread security vulnerabilities at the weapons laboratories has been ignored for far too long, and the work of the Cox Committee and intelligence officials at the Department has been invaluable in gaining the attention of the American public and in helping to focus the political will necessary to resolve these problems. Nonetheless, there have been many attempts to take the valuable coin of damaging new information and decrease its value by manufacturing its counterfeit, innuendo; possible damage has been minted as probable disaster; workaday delay and bureaucratic confusion have been cast as diabolical conspiracies. Enough is enough.

Fundamental change in DOE's institutional culture—including the ingrained attitudes toward security among personnel of the weapons laboratories—will be just as important as organizational redesign. The members of the Special Investigative Panel have never witnessed a bureaucratic culture so thoroughly saturated with cynicism and disregard for authority. Never before has this panel found such a cavalier attitude toward one of the most serious responsibilities in the federal government—control of the design information relating to nuclear weapons. Particularly egregious have been the failures to enforce cyber security measures to protect and control important nuclear weapons design information. Never before has the panel found an agency with the bureaucratic insolence to dispute, delay, and resist implementation of a Presidential directive on security as DOE's bureaucracy tried to do to the Presidential Decision Directive No. 61 in February 1998.

The best nuclear weapons expertise in the US Government resides at the national weapons labs, and the Intelligence Community should better use this asset. For years, the PFIAB has been keen on honing the Intelligence Community's analytic effectiveness on a wide array of nonproliferation areas, including nuclear weapons. We believe that the DOE Office of Intelligence, particularly its analytic component, has historically been an impediment to this goal because of its ineffective attempts to manage the labs' analysis. The office's mission and size (about 70 people) is totally out of step with the Department's intelligence

needs. A streamlined intelligence liaison body, much like Department of Treasury's Office of Intelligence Support—which numbers about 20 people, including a 24-hour watch team—would be far more appropriate. It should concentrate on making the Intelligence Community, which has the preponderance of overall analytic experience, more effective in fulfilling the DOE's analysis and collection requirements.

Root Causes

The sources of DOE's difficulties in both overseeing scientific research and maintaining security are numerous and deep. The Special Investigative Panel primarily focused its inquiry on the areas within DOE where the tension between science and security is most critical: the nuclear weapons laboratories.¹ To a lesser extent, the panel examined security issues in other areas of DOE and broad organizational issues that have had a bearing on the functioning of the laboratories.

Inherent in the work of the weapons laboratories, of course, is the basic tension between scientific inquiry, which thrives on freewheeling searches for and wide dissemination of information, and governmental secrecy, which requires just the opposite. But the historical context in which the labs were created and thrived has also figured into their subsequent problems with security.

Big, Byzantine, and Bewildering Bureaucracy

DOE is not one of the federal government's largest agencies in absolute terms, but its organizational structure is widely regarded as one of the most confusing. That structure is another legacy of its origins, and it has made the creation, implementation, coordination, and enforcement of consistent policies very difficult over the years.

The effort to develop the atomic bomb was managed through an unlikely collaboration of the Manhattan Engineering District of the US Army Corps of Engineers (hence the name, "the Manhattan Project") and the University of

California—two vastly dissimilar organizations in both culture and mission. The current form of the Department took shape in the first year of the Carter Administration through the merging of more than 40 different government agencies and organizations, an event from which it has arguably never recovered.

The newly created DOE subsumed the Federal Energy Administration, the Energy Research and Development Administration (ERDA), the Federal Power Commission, and components and programs of several other government agencies. Included were the nuclear weapons research laboratories that were part of the ERDA and, formerly, of the Atomic Energy Commission.

Many of these agencies and organizations have continued to operate under the DOE umbrella with the same organizational structure that they had before joining the Department.

Even before the new Department was created, concerns were raised about how high the nuclear weapons-related operations would rank among the competing priorities of such a large bureaucracy. A study of the issue completed in the last year of the Ford Administration considered three alternatives: shifting the weapons operations to the Department of Defense, creating a new freestanding agency, or keeping the program within ERDA—the options still being discussed more than 20 years later. As one critic of the DOE plan told *The Washington Post*, “Under the AEC, weapons was half the program. Under ERDA, it was one-sixth. Under DOE, it will be one-tenth. It isn’t getting the attention it deserves.” Although the proportions cited by that critic would prove to be inaccurate, he accurately spotted the direction of the trend.

Lack of Accountability

Depending on the issue at hand, a line worker in a DOE facility might be responsible to DOE headquarters in Washington, a manager in a field office in another state, a private contractor assigned to a DOE project, a research team leader from academia, or a lab director on another floor of the

worker’s building. For example, prior to Secretary Richardson’s restructuring initiative earlier this year, a single laboratory, Sandia, was managed or accountable to nine DOE security organizations.

Last year, after years of reports highlighting the problem of confused lines of authority, DOE was still unable to ensure the effectiveness of security measures because of its inability to hold personnel accountable. A 1998 report lamented that, “short of wholesale contract termination, there did not appear to be adequate penalty/reward systems to ensure effective day-to-day security oversight at the contractor level.”²

The problem is not only the diffuse nature of authority and accountability in the Department, but it is also the dynamic and often informal character of the authority that does exist. The inherently unpredictable outcomes of major experiments, the fluid missions of research teams, the mobility of individual researchers, the internal competition among laboratories, the ebb and flow of the academic community, the setting and onset of project deadlines, the cyclical nature of the federal budgeting process, and the shifting imperatives of energy and security policies dictated from the White House and Congress all contribute to volatility in the Department’s work force and an inability to give the weapons-related functions the priority they deserved. Newcomers, as a result, have an exceedingly hard time when they are assimilated; incumbents have a hard time in trying to administer consistent policies; and outsiders have a hard time divining departmental performance and which leaders and factions are credible. Such problems are not new to government organizations, but DOE’s accountability vacuum has only exacerbated them.

Management and security problems have recurred so frequently that they have resulted in nonstop reform initiatives, external reviews, and changes in policy direction. As one observer noted in *Science* magazine in 1994, “Every administration sets up a panel to review the national labs. The problem is that nothing is done.” The constant managerial turnover over the years has generated

nearly continuous structural reorganizations and repeated security policy reversals. Over the last 12 years, DOE has averaged some kind of major departmental shakeup every two to three years. During that time, security and counterintelligence responsibilities have been “punted” from one office to the next.

Culture and Attitudes

One facet of the culture mentioned more than others is an arrogance borne of the simple fact that nuclear researchers specialize in one of the world’s most advanced, challenging, and esoteric fields of knowledge. Nuclear physicists, by definition, are required to think in literally other dimensions not accessible to laymen. Thus it is not surprising that they might bridle under the restraints and regulations of administrators and bureaucrats who do not entirely comprehend the precise nature of the operation being managed.

Operating within a large, complex bureaucracy with transient leaders would tend to only accentuate a scientist’s sense of intellectual superiority: if administrators have little more than a vague sense of the contours of a research project, they are likely to have little basis to know which rules and regulations constitute unreasonable burdens on the researchers’ activities.

With respect to at least some security issues, the potential for conflicts over priorities is obvious. For example, how are security officials to weigh the risks of unauthorized disclosures during international exchanges if they have only a general familiarity with the cryptic jargon used by the scientists who might participate?

The prevailing culture of the weapons labs is widely perceived as contributing to security and counterintelligence problems. At the very least, restoring public confidence in the ability of the labs to protect nuclear secrets will require a thorough reappraisal of the culture within them.

Changing Times, Changing Missions

The external pressures placed on DOE in general, and the weapons labs in particular, are also worth noting. For more than 50 years, America’s nuclear researchers have operated in a maelstrom of shifting and often contradictory attitudes. In the immediate aftermath of World War II, nuclear discoveries were simultaneously hailed as a destructive scourge and a panacea for a wide array of mankind’s problems. The production of nuclear arms was regarded during the 1950s and 1960s as one of the best indices of international power and the strength of the nation’s military deterrent.

During the 1970s, the nation’s leadership turned to nuclear researchers for solutions to the energy crisis at the same time that the general public was becoming more alarmed about the nuclear buildup and the environmental implications of nuclear facilities.

During the past 20 years, some in Congress have repeatedly called for the dissolution of the Department of Energy, which has undoubtedly been a distraction to those trying to make long-term decisions affecting the scope and direction of the research at the labs. And in the aftermath of the Cold War, the Congress has looked to the nation’s nuclear weapons labs to help in stabilizing or dismantling nuclear stockpiles in other nations.

Each time that the nation’s leadership has made a major change in the Department’s priorities or added another mission, it has placed additional pressure on a government agency already struggling to preserve and expand one of its most challenging historical roles: guarantor of the safety, security, and reliability of the nation’s nuclear weapons.

Recurring Vulnerabilities

During the past 20 years, six DOE security issues have received the most scrutiny and criticism from both internal and external reviewers: long-term security planning and policy implementation; physical security over facilities and property; screening and monitoring of personnel; protection

of classified and sensitive information, particularly information that is stored electronically in the Department's computers; accounting for nuclear materials; and the foreign visitors' programs.

Management and Planning

Management of security and counterintelligence has suffered from chronic problems since the creation of the Department of Energy in 1977. During the past decade, the mismatch between DOE's security programs and the severity of the threats faced by the Department grew more pronounced. While the number of nations possessing, developing, or seeking weapons of mass destruction continued to rise, America's reliance on foreign scientists and engineers dramatically increased, and warnings mounted about the espionage goals of other nations, and DOE spending on safeguards and security decreased by roughly one-third.³

The widening gap between the level of security and the severity of the threat resulted in cases where sensitive nuclear weapons information was certainly lost to espionage. In countless other instances, such information was left vulnerable to theft or duplication for long periods, and the extent to which these serious lapses may have damaged American security is incalculable. DOE's failure to respond to warnings from its own analysts, much less independent sources, underscores the depth of its managerial weakness and inability to implement legitimate policies regarding well-founded threats.

A Sample of Security Issues

Management and Planning

- *Decentralized decisionmaking undermines consistency of policies.*
- *Lack of control of security budget has allowed diversion of funds to other priorities.*
- *Department leaders with little experience in security and intelligence.*
- *Lack of accountability.*

Physical Security

- *Training insufficient for some security personnel.*
- *Nuclear materials stored in aging buildings not designed for containment purposes.*
- *Recurring problems involving lost or stolen property.*
- *Poor management results in unnecessary training and purchasing costs.*

Personnel Security Clearances

- *Extended lags in obtaining clearances, reinvestigating backgrounds, and terminating clearance privileges for former employees.*
- *Some contractors not adequately investigated or subject to drug and substance abuse policies.*
- *Lack of uniform procedures and accurate data.*
- *Inadequate pre-employment screening.*
- *More clearances granted than necessary.*

Protection of Classified Information

- *Poor labeling and tracking of computer media containing classified information.*
- *Problems with lax enforcement of password policies.*
- *Network, e-mail, and Internet connections make transfer of large amounts of data easier.*

Accounting for Nuclear Materials

- *Chronic problems in devising and operating an accurate accounting system of tracking stocks and flows of nuclear materials.*

Foreign Visitors

- *Weak systems for tracking visits and screening backgrounds of visiting scientists.*
- *Decentralization makes monitoring of discussions on sensitive topics difficult.*

During the mid-1980s, the predominant concern of DOE officials was improving the physical security of the nuclear weapons laboratories and plants. Following a January 1983 report⁴ that outlined vulnerabilities of the weapons labs to terrorism, the Department embarked on a five-year program of construction and purchases that would see its overall safeguards and security budget roughly double and its spending on upgrades nearly triple. Included was money for additional guards, security training, helicopters, fortified guard towers, vehicle barriers, emergency planning, and advanced alarm systems.⁵

Improving physical security in a wide array of nuclear weapons facilities, whose replacement value was an estimated \$100 billion,⁶ proved to be difficult. Reports through the late 1980s and early 1990s continued to highlight deficiencies in the management of physical security.

In the late 1980s, priorities began to shift somewhat. Listening devices were discovered in weapons-related facilities,⁷ and a 1990 study advised the Department leadership of an intensifying threat from foreign espionage. Less and less able to rely on the former Soviet Union to supply technology and resources, an increasing number of states embarked on campaigns to bridge the economic and technological gap with the United States by developing indigenous capabilities in high-technology areas. The study noted that the freer movement of goods, services, and information in a less hostile world “intensified the prospects and opportunities for espionage as missing pieces of critically needed information became more easily identified.”⁸

An intelligence report further highlighted the changing foreign threat to the labs by noting that “new threats are emerging from nontraditional adversaries who target issues key to US national security. DOE facilities and personnel remain priority targets for hostile intelligence collection.”⁹ Anecdotal evidence corroborates, and intelligence assessments agree, that foreign powers stepped up targeting of DOE during the early 1990s (see the classified Appendix). While this threat may

have been taken seriously at the highest levels of the DOE, it was not uniform throughout the Department.

A former FBI senior official noted in discussions with the PFIAB investigative panel that DOE lab scientists during these years appeared naive about the level of sophistication of the nontraditional threat posed by Chinese intelligence collection. The trend in openness to foreign visitors and visits does not indicate any sense of heightened wariness. A 1997 GAO report concluded that, from mid-1988 to the mid-1990s, the number of foreign visitors to key weapons labs increased from 3,800 to 5,900 annually, and sensitive country visitors increased from 500 to more than 1,600.¹⁰ Meanwhile, the DOE budget for counterintelligence was in near-constant decline.

As noted in the previous chapter, federal officials in charge of oversight of nuclear weapons laboratories have historically allowed decision-making on basic aspects of security to be decentralized and diffuse. With their budget spread piecemeal throughout a number of offices, security and counterintelligence officials often found themselves with a weak voice in internal bureaucratic battles and an inability to muster the authority to accomplish its goals. Indeed, an excerpt from a history of the early years of the Atomic Energy Commission reads much like recent studies:

*Admiral Gingrich, who had just resigned as director of security [in 1949], had expressed to the Joint Committee [on Atomic Energy] a lack of confidence in the Commission’s security program. Gingrich complained that decentralization of administrative functions to the field offices had left him with little more than a staff function at headquarters; even there, he said, he did not control all the activities that seemed properly to belong to the director of security.*¹¹

More than 30 years later, decentralization still posed a problem for security managers. An internal DOE report in 1990 found that the Department lacked a comprehensive approach to management

of threats and dissemination of information about them.¹² An annual DOE report in 1992 found that security “has suffered from a lack of management focus and inconsistent procedural execution throughout the DOE complex. The result is that personnel are seldom held responsible for their disregard, either intentional or unintentional, of security requirements.”¹³

The counterintelligence effort at DOE in the late 1980s and mid-1990s was in its infancy and grossly under-funded stage. Although the Department could have filled its gap in some areas, such as counterintelligence information, through cooperation with the broader Intelligence Community, PFIAB research and interviews indicate that DOE headquarters’ relationship with the FBI—the United States’ primary domestic CI organization—was strained at best.

In 1998, DOE requested an FBI agent detailee to assist in developing a CI program, but the agent found that DOE failed to provide management support or access to senior DOE decision-makers. A formal relationship with the FBI was apparently not established until 1992: a Memorandum of Understanding between the FBI and DOE on respective responsibilities concerning the coordination and conduct of CI activities in the United States. However, in 1994 two FBI detailees assigned to DOE complained about their limited access and were pulled back to the FBI because of a “lack of control of the CI program by DOE Headquarters, which resulted in futile attempts to better manage the issue of foreign visitors at the laboratories.”¹⁴

The haphazard assortment of agencies and missions folded into DOE has become so confusing as to become a running joke within the institution. In the course of the panel’s research and interviews, rare were the senior officials who expressed any sort of confidence in their understanding of the extent of the agency’s operations, facilities, or procedures. Time and again, PFIAB panel members posed the elementary questions to senior DOE officials. To whom do you report? To whom

are you accountable? The answer, invariably, was, “It depends.”

DOE’s relationship with the broader Intelligence Community was not well defined until the mid-1990s. Coordination between DOE CI elements and the broader Intelligence Community, according to a 1992 intelligence report, was hampered from the 1980s through the early 1990s by DOE managers’ inadequate understanding of the Intelligence Community.¹⁵ The Department did not become a core member of the National Counterintelligence Policy Board (established in 1994 under PDD-24) until 1997.

Over much of the past decade, rather than a heightened sensitivity to espionage threats recognized widely throughout the Intelligence Community, DOE lab officials have operated in an environment that allowed them to be sanguine, if not skeptical. Numerous DOE officials interviewed by the PFIAB panel stated that they believed that the threat perception was weakened further during the administration of Secretary O’Leary, who advanced the labs openness policies and downgraded security as an issue by terminating some security programs instituted by her predecessor.

Even when the CI budget was expanded in the late 1990s, the expenditures fell short of the projected increases. In Fiscal Year 1997, for example, DOE’s CI budget was \$3.7 million, but the actual expenditures on CI were only two-thirds of that level, \$2.3 million. Shortly before the 1997 GAO and FBI reports on DOE’s counterintelligence posture were issued, DOE began instituting changes to beef up its counterintelligence and foreign intelligence analytic capabilities.¹⁶

When DOE did devote its considerable resources to security, it too often faltered in implementation. A report sent to the Secretary in January 1994 noted “growing confusion within the Department with respect to Headquarters’ guidance for safeguards and security. At this time, there is no single office at Headquarters responsible for the safeguards and security program. Most recently, a number

of program offices have substantially expanded their safeguards and security staff to office-size organizations. These multiple safeguards and security offices have resulted in duplication of guidance, unnecessary requests for information and clarification, and inefficient program execution. Unchecked, this counterproductive tendency threatens the success of the overall safeguards and security effort.”¹⁷

A 1996 DOE Inspector General report found that security personnel at the weapons programs had purchased and stockpiled far more firepower—ranging from handguns and rifles to submachine guns and grenade launchers—than could ever be used in an actual emergency. The Oak Ridge facilities had more than three weapons per armed security officer—on and off duty; Los Alamos National Laboratory had more than four.¹⁸

Around the same time, GAO security audits of the research laboratories at these sites found lax procedures for issuing access passes to secure areas, inadequate prescreening of the more than 1,500 visitors from sensitive countries that visited the weapons laboratories annually, and poor tracking of the content of discussions with foreign visitors. The implication: foreign agents could probably not shoot their way past the concertina wires and bolted doors to seize secrets from US weapons laboratories, but they would not need to do so. They could probably apply for an access pass, walk in the front door, and strike up a conversation.

Physical Security

The physical security of the Department of Energy’s weapons-related programs is roughly divided into two essential functions: tracking and control over the property and equipment within the weapons-related laboratories and keeping unwarranted intruders out, often referred to as the realm of “guns, guards, and gates.”

The general approach to security, of course, was defined by the emphasis on secrecy associated with nuclear weapons program during World War

II. Los Alamos National Laboratory was created as a “closed city”—a community with a high degree of self-sufficiency, clearly defined and protected boundaries, and a minimum of ingress from and egress to the outer world. Although the community is no longer “closed,” the weapons laboratories at Los Alamos, like those at the other national laboratories, still retain formidable physical protections and barriers. In examining the history of the laboratories, the panel found only a few instances where an outsider could successfully penetrate the grounds of an operation by destruction of a physical safeguard or direct violent assault.

In visits to several of the weapons laboratories, the members of the Special Investigative Panel were impressed by the great amount of attention and investment devoted to perimeter control, weaponry, and security of building entrances and exits. Indeed, one cannot help but be struck by the forbidding and formidable garrison-type atmosphere that is prevalent at many of the facilities: barbed wire, chain-link fences, electronic sensors, and surveillance cameras. Further, the panel recognizes that the labs themselves have developed and produced some of the most sophisticated technical security devices in the world. Nonetheless, DOE reports and external reviews since at least 1984 have continued to raise concerns about aging security systems.¹⁹

Management of the secure environments at the laboratories has posed more serious problems. As noted earlier, DOE may be spending too much money in some areas, buying more weapons than could conceivably be used in an emergency situation. In other cases, it may be spending too little. Budget cuts in the early and mid-1990s led to 40- to 50-percent declines in officer strength and over-reliance on local law enforcement. Resources became so low that normal protective force operations required “the use of overtime scheduling to accomplish routine site protection.”²⁰ GAO has found an assortment of problems at Los Alamos over the past decade: security personnel failed basic tests in such tasks as firing weapons, using a baton, or handcuffing a suspect and inaccurate and

incomplete records were kept on security training.²¹ Other DOE facilities have had substantial problems in management of physical property:

- In 1990, Lawrence Livermore Laboratory could not account for 16 percent of its inventory of government equipment, acquired at a cost of \$18.6 million.²²
- In 1993, DOE sold 57 components of nuclear reprocessing equipment and associated documents, including blueprints, to an Idaho salvage dealer. Much of what was sold was subsequently found to be potentially useful to any nation attempting to develop or advance its own reprocessing operation.²³
- Following a GAO report in 1994, which found that the Rocky Flats facility was unable to account for large pieces of equipment such as forklifts and a semi-trailer, some \$21 million in inventory was written off.²⁴

DOE had begun to consolidate its growing stockpile of sensitive nuclear material by 1992, but a 1997 DOE report to the Secretary found that significant quantities of the material “remain in aging buildings and structures, ranging in age from 12 to 50 years that were never intended for use as storage facilities for extended periods.”²⁵

Screening and Monitoring of Personnel

Insider threats to security have been a chronic problem at the nation’s weapons laboratories. From the earliest years, the importance of the labs’ missions and their decentralized structure have had an uneasy coexistence with the need for thorough background investigations of researchers and personnel needing access to sensitive areas and information.

In 1947, the incoming director of security for the AEC was greeted with a backlog of more than 13,000 background investigations and a process where clearances had been dispersed to field offices that operated with few formal guidelines.²⁶

Forty years later, GAO found that the backlog of personnel security investigations had increased

more than nine-fold, to more than 120,000. Moreover, many clearances recorded as valid in the Department’s records should have been terminated years before.²⁷

Even after DOE discovered listening devices in some of its weapons laboratories, security audits found that thousands of “Q” clearances were being given to inappropriate personnel.²⁸

The research of the PFIAB panel found that problems with personnel security clearances, while mitigated in some aspects, have persisted to an alarming degree. From the mid-1980s through the mid-1990s, the DOE Inspector General repeatedly warned Department officials that personnel were receiving clearances that were much higher than warranted and that outdated clearances were not being withdrawn on a timely basis. The issue became more urgent with the discovery of a clandestine surveillance device at a nuclear facility.²⁹

DOE Inspector General reports in 1990 and 1991 found that one of the weapons laboratories had granted “Q” clearances (which provide access to US Government nuclear weapons data) to more than 2,000 employees who did not need access to classified information.³⁰ A 1992 report to the Secretary of Energy noted that “DOE grants clearances requested by its three major defense program sponsored labs based on lab policies to clear all employees regardless of whether actual access to classified interests is required for job performance.”³¹

Three years later, a review of personnel security informed the Secretary that there were “individuals who held security clearances for convenience only and limited security clearances to those individuals requiring direct access to classified matter or [special nuclear materials] to perform official duties.”³²

More recent evidence is no more reassuring. A counterintelligence investigation at a nuclear facility discovered that the subject of an inquiry had been granted a “Q” clearance simply to avoid

the delay caused by the normal processing of a visit.³³ During that same year, an illegal telephone wiretap was discovered at the same lab. The employee who installed it confessed but was not prosecuted by the government.³⁴

Protection of Classified and Sensitive Information

Two vulnerabilities regarding classified and sensitive information at DOE have recurred repeatedly throughout the past 20 years: inappropriate release of classified information, either directly through inadvertence or indirectly through improper declassification; and the increasing mobility of classified and sensitive information through electronic media, such as computers.

As computers have progressed from large mainframes of the 1950s and 1960s to desktop models in the 1980s and decentralized networks in the 1990s, it has become progressively easier for individuals to retrieve and transport large amounts of data from one location to another. This has presented an obvious problem for secure environments. GAO found in 1991 that DOE inspections revealed more than 220 security weaknesses in computer systems across 16 facilities. Examples included a lack of management plans, inadequate access controls, and failures to test for compliance with security procedures.³⁵

As a 1996 DOE report to the President said, “adversaries no longer have to scale a fence, defeat sensors, or bypass armed guards to steal nuclear or leading-edge ‘know-how’ or to shut down our critical infrastructure. They merely have to defeat the less ominous obstacles of cyber-defense.”³⁶

Computer systems at some DOE facilities were so easy to access that even Department analysts likened them to “automatic teller machines, [allowing] unauthorized withdrawals at our nation’s expense.”

DOE’s cyber defenses were, in fact, found to be “less ominous obstacles.” In 1994, an internal DOE review found that despite security improvement “users of unclassified computers continue to compromise classified information due to ongoing inadequacies in user awareness training, adherence to procedures, enforcement of security policies, and DOE and [lab] line management oversight.”³⁷ Also in 1994, a report to the Energy Secretary cited five areas of concern: “failure to properly accredit systems processing classified information, lack of controls to provide access authorities and proper password management; no configuration management; improper labeling of magnetic media; and failure to perform management reviews.”³⁸

Apparently, the warnings were to no avail. A year later, the annual report to the Secretary noted, “Overall, findings and surveys, much like last year, continue to reflect deficiencies in self-inspections and procedural requirements or inappropriate or inadequate site guidance ... In the area of classified matter protection and control, like last year, marking, accountability, protection, and storage deficiencies are most numerous.”³⁹

Some reports made extra efforts to puncture through the fog of bureaucratic language. A 1995 report to the President noted, “By placing sensitive information on information systems, we increase the likelihood that inimitable interests, external and internal, will treat those systems as virtual automatic teller machines, making unauthorized withdrawals at our nation’s expenses.” Indeed, a report found security breaches at one of the major weapons facility in which documents with unclassified but sensitive information “were found to be stored on systems that were readily accessible to anyone with Internet access.”⁴⁰ In other instances, personnel were found to be sending classified information to outsiders via an unclassified e-mail system.⁴¹

In 1986, the DOE Office of Safeguards and Quality Assessment issued an inspection report on a weapons lab that warned of shortcomings in computer security and noted that the “ability of

[a] user to deliberately declassify a classified file without detection and move classified information from the secure partition to the open partition can be made available to any authorized user either on or off site.”⁴² The warning turned out to be on the mark. In April 2001, Energy Secretary Bill Richardson issued the statement, “While I cannot comment on the specifics, I can confirm that classified nuclear weapons computer codes at Los Alamos were transferred to an unclassified computer system. This kind of egregious security breach is absolutely unacceptable.”

Even though the hard evidence points to only sporadic penetrations of the labs by foreign intelligence services, volumes of sensitive and classified information may have been lost over the years—via discarded or purloined documents, uninformed and often improperly vetted employees, and a maze of uncontrolled computer links. In one recent case discovered by PFIAB, lab officials initially refused to rectify a security vulnerability because “no probability is assigned to [a loss of sensitive information], just the allegation that it is possible.”⁴³

As recent as last year’s annual DOE report to the President, security analysts were finding “numerous incidents of classified information being placed on unclassified systems, including several since the development of a corrective action plan in July 1998.”⁴⁴

Foreign Visitors and Assignments Program

True to the tradition of international partnership molded by the experiences of the Manhattan Project, the weapons labs have remained a reservoir of the best international scientific talent. Recent examples abound: a supercomputing team from Oak Ridge National Lab, made up of three PRC citizens and a Hungarian, recently won the Gordon Bell Prize; a Bulgarian and a Canadian, both world-class scientists, are helping Lawrence Livermore National Lab solve problems in fluid dynamics; a Spanish scientist, also at Livermore, is collaborating with colleagues on laser propagation.

For more than a decade, the increasing prominence of foreign visitors in the weapons labs has increased concern about security risks. The PFIAB found that, as early as 1985, the DCI raised concerns with the Energy Secretary about the foreign visitors’ program. A year later, researchers conducting internal DOE review could find only scant data on the number and composition of foreign nationals at the weapons labs. Although intelligence officials drafted suggestions for DOE’s foreign visitor control program, PFIAB found little evidence of reform efforts until the tenure of Secretary Watkins.

A 1988 GAO report cited DOE for failing “to obtain timely and adequate information on foreign visitors before allowing them access to the laboratories.” The GAO found three cases where DOE allowed visitors with questionable backgrounds—possible foreign agents—access to the labs. In addition, the GAO found that about 10 percent of 637 visitors from sensitive countries were associated with foreign organizations suspected of conducting nuclear weapons activities, but DOE did not request background data on them prior to their visit. DOE also had not conducted its own review of the visit and assignment program at the weapons labs despite the DOE requirement to conduct audits or reviews at a minimum of every five years. Moreover, GAO reported that few post-visit or host reports required by DOE Order 12402 were submitted within 30 days of the visitors’ departure, and some were never completed.⁴⁵

In 1989, DOE revised its foreign visitor policy and commissioned an external study on the extent and significance of the foreign visitor problem. DOE’s effort to track and vet visitors, however, still lagged the expansion of the visitor program, allowing foreigners with suspicious backgrounds to gain access to weapons facilities. A study published in June 1990 indicated DOE had a “crippling lack of essential data, most notably no centralized, retrievable listing of foreign national visitors to government facilities.”⁴⁶

By September 1992, DOE had instituted Visitor Assignment Management System (VAMS)

databases to track visitors and assignees requesting to visit DOE. The system, however, failed to provide links between the labs that could be used for CI analysis and crosschecking of prospective visitors. Moreover, labs frequently did not even use the database and failed to enter visitor information. Instead, each lab independently developed its own computer program.

Reviews of security determined that, despite an increase of more than 50 percent in foreign visits to the labs from the mid-1980s to the mid-1990s, DOE controls on foreign visitors actually weakened in two critical areas: screening for visitors that may pose security risks and monitoring the content of discussions that might disclose classified information.

In 1994, DOE headquarters delegated greater authority to approve non-sensitive country visitors to the laboratories, approving a partial exception for Los Alamos and Sandia National Laboratories to forego background checks to help “reduce costs and processing backlogs.” This resulted in almost automatic approval of some foreign visitors and fewer background checks. The FBI and GAO subsequently found that “questionable visitors, including suspected foreign intelligence agents, had access to the laboratories without DOE and/or laboratory officials’ advance knowledge of the visitors’ backgrounds.”⁴⁷

Changes in records checks over the past decade also made it easier for individuals from sensitive countries to gain access to the laboratories. In 1988, for example, all visitors from Communist countries required records checks regardless of the purpose of the visit. By 1996, records checks were required for visitors from only sensitive countries who visited secure areas or discussed sensitive subjects.

In 1996 an internal DOE task force determined that the Department’s definitions of sensitive topics were not specific enough to be useful. The task force directed the DOE office of intelligence to develop a new methodology for defining sensitive topics, but did not set a due date. The 1996 group

also called for a Deputy Secretary–level review of foreign visits and assignments to be completed by June 1997.⁴⁸ The PFIAB panel found no evidence to suggest that these tasks were accomplished.

In 1997, GAO found that DOE lacked clear criteria for identifying visits that involve sensitive subjects; US scientists may have discussed sensitive subjects with foreign nationals without DOE’s knowledge or approval; and the Department’s counterintelligence program had failed to produce comprehensive threat assessments that would identify likely facilities, technologies, and programs targeted by foreign intelligence.⁴⁹ The study found that record checks were still not regularly conducted on foreign visitors from sensitive countries.⁵⁰ Last year, 7,600 foreign scientists visited the weapons labs.⁵¹ Of that total, about 34 percent were from countries that are designated “sensitive” by the Department of Energy—meaning they represent a hostile intelligence threat. The GAO reported last year that foreign nationals had been allowed after-hours and unescorted access to buildings.⁵²

Responsibility

While cultural, structural, and historical problems have all figured into the management and security and counterintelligence failures of DOE, they should not be construed as an excuse for the deplorable irresponsibility within the agency, the pattern of inaction from those charged with implementation of policies, or the inconsistency of those in leadership positions. The panel identified numerous instances in which individuals were presented with glaring problems yet responded with foot-dragging, finger-pointing, bland reassurances, obfuscation, and even misrepresentations.

The record of inattention and “false start” reforms goes back to the beginning of DOE. There have been several Presidents; National Security Advisors; Energy Secretaries, Deputy Secretaries, Assistant Secretaries, and Lab Directors; DOE Office Directors and Lab managers; and Energy Department bureaucrats and Lab scientists who all must shoulder the responsibility and accountability.

As noted above, severe lapses in the security of the nation's most critical technology, data, and materials were manifest at the creation of the DOE more than 20 years ago. Many, if not most, of the problems were identified repeatedly. Still, reforms flagged amid a lack of discipline and accountability. The fact that virtually every one of those problems persisted—indeed, many of the problems still exist—indicates a lack of sufficient attention by every President, Energy Secretary, and Congress.

This determination is in no way a capitulation to the standard of “everyone is responsible, therefore no one is responsible.” Quite the contrary, even a casual reading of the open-source reports on the Department's problems presents one with a compelling narrative of incompetence that should have merited the aggressive action of the nation's leadership. Few transgressions could violate the national trust more than inattention to one's direct responsibility for controlling the technology of weapons of mass destruction.

The PFIAB was not empowered, nor was it charged, to make determinations of whether specific acts of espionage or malfeasance occurred regarding alleged security lapses at the weapons labs. The PFIAB also was not tasked to issue performance appraisals of the various Presidents, Energy Secretaries, or members of the Congressional leadership during their respective terms in office. However, an inquiry into the extent to which the system of administrative accountability and responsibility broke down at various times in history has been necessary to fulfill our charter. In fairness, we have tried to examine the nature of the security problems at DOE's weapons labs in many respects and at many levels, ranging from the circumstances of individuals and the dynamics of group behavior to the effectiveness of mid-level management, the clarity of the laws and regulations affecting the Department, and the effectiveness of leadership initiatives.

The Record of the Clinton Team

To its credit, in the past two years the Clinton Administration has proposed and begun to implement some of the most far-reaching reforms in DOE's history. The 1998 Presidential Decision Directive on DOE counterintelligence (PDD-61) and Secretary Richardson's initiatives are both substantial and positive steps.

However, the speed and sweep of the Administration's ongoing response does not absolve it of its responsibility in years past. At the outset of the Clinton Administration—in 1993, when it inherited responsibility for DOE and the glaring record of mismanagement of the weapons laboratories—the incoming leadership did not give the security and counterintelligence problems at the labs the priority and attention they warranted. It will be incumbent on the DOE transition team for the incoming administration in 2001 to pay particular heed to these issues.

While the track record of previous administrations' responses to DOE's problems is mixed, the panel members believe that the gravity of the security and counterintelligence mismanagement at the Department will, and should, overshadow post facto claims of due diligence by any administration—including the current one. Asserting that the degree of failure or success with DOE from one administration to the next is relative is, one might say, gilding a fig leaf.

Each successive administration had more evidence of DOE's systemic failures in hand: the Reagan Administration arrived to find several years' worth of troubling evidence from the Carter, Ford, and Nixon years; the evidence had mounted higher by the time the Bush Administration took over; and even higher when the Clinton Administration came in. The Clinton Administration has acted forcefully, but it took pressure from below and outside the Administration to get the attention of

the leadership, and there is some evidence to raise questions about whether its actions came later than they should have, given the course of events that led the recent flurry of activity.

The 1995 “Walk-In” Document

In 1995, a US intelligence agency obtained information that has come to be called the “walk-in” document. This document is a classified PRC report that contains a discussion of various US nuclear warheads. The PFIAB has carefully reviewed this document, related information, and the circumstances surrounding its delivery. Serious questions remain as to when it was written, why it was written, and why it was provided to the United States. We need not resolve these questions. The document unquestionably contains some information that is still highly sensitive, including descriptions, in varying degrees of specificity, of technical characteristics of seven US thermonuclear warheads. This information had been widely available within the US nuclear weapons community, including the weapons labs, other parts of DOE, the Department of Defense, and private contractors, for more than a decade. For example, key technical information concerning the W-88 warhead had been available to numerous US Government and military entities since at least 1983 and could well have come from many organizations other than the weapons labs.

W-88 Investigation

Despite the disclosure of information concerning seven warheads, despite the potential that the source or sources of these disclosures were other than the bomb designers at the national weapons labs, and despite the potential that the disclosures occurred as early as 1982, only one investigation was initiated. That investigation focused on only one warhead—the W-88—only one category of potential sources—bomb designers at the national labs—and only a four-year window of opportunity. It should have been pursued in a more comprehensive manner. The allegations raised in the investigation should still be pursued vigorously,

and the inquiry should be fully explored regardless of the conclusions that may result.

The episode began as an administrative inquiry conducted by the DOE Office of Energy Intelligence, with limited assistance from the FBI. It developed into an FBI investigation, which is still under way today. Allegations concerning this case and related activities highlighted the need for improvements in the DOE’s counterintelligence program, led along the way to the issuance of a Presidential Decision Directive revamping the DOE’s counterintelligence program, formed a substantial part of the information underlying the Cox Committee’s conclusions on nuclear weapons information, and ultimately led, at least in part, to the President’s decision to ask this Board to evaluate security and counterintelligence at the DOE’s weapons labs.

It is not within the mandate of our review to solve the W-88 case or any other potential compromises of nuclear weapons information. Further, it is not within our mandate to conduct a comprehensive and conclusive evaluation of the handling of the W-88 investigation by the Department of Justice and FBI.

It is, however, explicitly within our mandate to identify additional steps that may need to be taken to address the security and counterintelligence threats to the weapons labs. Also, it is within our standing PFIAB obligation under Executive Order 12863 to assess the adequacy of counterintelligence activities beyond the labs. In this regard, what we have learned from our limited review of the W-88 case and other cases are significant lessons that extend well beyond these particular cases. These lessons relate directly to additional steps we believe must be taken to strengthen our safeguards against current security and foreign intelligence threats.

We have learned, for example, that under the current personnel security clearance system a person who is under FBI investigation for suspected counterintelligence activities may sometimes be granted a new or renewed clearance.

We also have learned that, although the written standards for granting a first clearance and for renewing an existing clearance may be identical, the actual practice that has developed—certainly within DOE and we strongly suspect elsewhere—is that clearance renewals will be granted on a lower standard. We find such inconsistency unacceptable. We think it appropriate for the National Security Council to review and resolve these issues.

We have also learned that the legal weapons designed to fight the counterintelligence battles of the 1970s have not necessarily been rigorously adapted to fight the counterintelligence battles of the 1990s (and beyond). For example, with the passage of more than 20 years since the enactment of the Foreign Intelligence Surveillance Act (FISA) of 1978, it may no longer be adequate to address the counterintelligence threats of the new millennium. We take no position on whether the statute itself needs to be changed. It may well still be sufficient. However, based on all of the information we have reviewed and the interviews we have conducted and without expressing a view as to the appropriateness of the DOJ decision in the W-88 case, we do believe that the DOJ may be applying the FISA in a manner that is too restrictive, particularly in light of the evolution of a very sophisticated counterintelligence threat and the ongoing revolution in information systems. We also are concerned by the lack of uniform application across the government of various other investigative tools, such as employee waivers that grant officials appropriate authority to monitor sensitive government computer systems.

Moreover, there does not exist today a systematic process to ensure that the competing interests of law enforcement and national security are appropriately balanced. Law enforcement, rightly so, is committed to building prosecutable cases. Leaving an espionage suspect in place to facilitate the gathering of more evidence often furthers this goal. The national security interest, in contrast, is often furthered by immediately removing a suspect from access to sensitive information to avoid additional compromises. Striking the proper balance is never easy. It is made all the

more difficult when there is no regular process to ensure that balance is struck. We have learned in our review that this difficult decision often is made by officials who either are too focused on the investigative details or are too unaware of the details to make a balanced decision. This is another matter deserving National Security Council attention.

PFIAB Evaluation of the Intelligence Community Damage Assessment

Following receipt of the “walk-in” document, CIA, DOE, Congress, and others conducted numerous analyses in an effort to determine the extent of the classified nuclear weapons information the PRC has acquired and the resultant threat to US national security. Opinions expressed in the media and elsewhere have ranged from one extreme to the other. On one end of the spectrum is the view that the Chinese have acquired very little classified information and can do little with it. On the other end is the view that the Chinese have nearly duplicated the W-88 warhead.

After reviewing the available intelligence and interviewing the major participants in many of these studies, we conclude that none of these extreme views holds water. For us, the most accurate assessment of China’s acquisition of classified US nuclear weapons information and the resultant threat to US national security is presented in the April 1999 Intelligence Community Damage Assessment. Written by a team of experts, this assessment was reviewed and endorsed by an independent panel of national security and nuclear weapons specialists, chaired by Admiral David Jeremiah. We substantially agree with the assessment’s analysis and endorse its key findings.

Presidential Decision Directive 61: Birth and Intent

In mid-1997, it became clear to an increasingly broader range of senior administration officials that DOE’s counterintelligence program was in serious trouble.⁵³ In late July 1997, DOE officials briefed the President’s National Security

Advisor, who concluded that, while the real magnitude and national security implications of the suspected espionage needed closer scrutiny, there was, nonetheless, a solid basis for taking steps to strengthen counterintelligence measures at the labs. He requested an independent CIA assessment of China's nuclear program and the impact of US nuclear information, and he directed that the National Counterintelligence Policy Board (NACIPB)⁵⁴ review the DOE counterintelligence program. In September 1997, the National Security Advisor received the CIA assessment, and the NACIPB reported back that it had found "systemic and serious CI and security problems at DOE [had] been well documented over at least a ten year period" and "few of the recommendations in the past studies [had] been implemented." The NACIPB made 25 recommendations to significantly restructure the DOE CI program; it also proposed that a Presidential Decision Directive or Executive Order be handed down to effect these changes.

At a meeting on 15 October, the Director of Central Intelligence (DCI) and the FBI Director discussed with Secretary Pena and his Deputy Secretary the need to reform the DOE CI program. The DCI and FBI Director sought to make clear that there was an urgent need to act immediately, and "despite all the studies conducted, experience over time [had] shown that DOE's structure and culture make reform difficult, if not impossible, from within." All agreed to develop an action plan that would serve as the basis for a Presidential Decision Directive (PDD). Several senior officials involved felt that the necessary reforms would—without the mandate of a Presidential directive—have little hope of overcoming the anticipated bureaucratic resistance, both at DOE headquarters and at the labs. There was a clear fear that, "if the Secretary spoke, the bureaucracy wouldn't listen; if the President spoke, the bureaucracy might at least listen."

During the winter of 1997, the NSC coordinated a draft PDD among the many agencies and departments involved. Serious disagreements arose over several issues, particularly the creation of

independent reporting lines to the Secretary for the Intelligence and Counterintelligence Offices. Also at issue was the subordination of the CI officers at the labs. Much of the resistance stemmed simply from individuals interested in preserving their turf won in previous DOE bureaucratic battles. After much bureaucratic maneuvering and even vicious infighting, these issues were finally resolved, or so it seemed; and on 11 February 1998, the President signed and issued the directive as PDD-61.

The full PDD remains classified. In our view, among the most significant of the 13 initiatives directed by PDD-61 are:

- The CI and foreign intelligence (FI) elements would be reconfigured into two independent offices and report directly to the Secretary of Energy.
- The Director of the new Office of CI (OCI) would be a senior executive from the FBI and would have direct access to the Secretary of Energy, the DCI, and the Director of the FBI.
- Existing DOE contracts with the labs would be amended to include CI program goals and objectives and performance measures to evaluate compliance with these contractual obligations, and CI personnel assigned to the labs would have direct access to the lab directors and would concurrently report to the Director OCI.
- Ninety days after his arrival, the incoming Director OCI would prepare a report for the Secretary of Energy that would address progress on the initiative, a strategic plan for achieving long-term goals, and recommendations on whether and to what extent other organizational changes may be necessary to strengthen CI.
- Within 120 days, the Secretary of Energy would advise the Assistant to the President for National Security Affairs on the actions taken and specific remedies designed to implement this directive.

On 1 April 1998, a senior executive from the FBI assumed his duties as the Director of the OCI and began his 90-day study. He completed and forwarded the study to the Secretary of Energy on 1 July, the day after Secretary Pena resigned. The Acting Secretary, Elizabeth A. Moler, led a

review of the study and its recommendations. On 18 August, Secretary Richardson was sworn in. On 13 November, Richardson submitted the CI Action Plan required by the PDD to the National Security Advisor. He also met with lab CI Directors and DOE headquarters CI and Intelligence staff to discuss the implementation plan. The implementation plan continued to be developed by his staff, and the completed plan was delivered to Secretary Richardson on 3 February 1999. It was issued to the labs on 4 March.

Timeliness of PDD-61

Criticism has been raised that the PDD took too long to issue and has taken too long to implement. Although the current National Security Advisor was briefed on counterintelligence concerns by DOE officials in April 1996, we are not convinced that the briefing provided a sufficient basis to require initiation of a broad Presidential directive at that time. We are convinced, however, that the July 1997 briefing, which we are persuaded was much more comprehensive, was sufficient to warrant aggressive White House action. We believe that, while the resulting PDD was developed and issued within a customary amount of time, these issues had such national security gravity that it should have been handled with more dispatch. It is not surprising that there were disagreements over various issues. It is very disturbing that the DOE bureaucracy dug in its heels so deeply in resisting clearly needed reform. In fact, we believe that the NACIPB, created by PDD in 1994, was a critical factor in ram-rodding the PDD through to signature. Before 1994, there was no real structure or effective process for handling these kinds of issues in a methodical way. Had the new structure not been in place and working, we doubt if the PDD would have made it.

With regard to timeliness of implementation, we have far greater concern. The PFIAB recognized that senior DOE officials would require some time to evaluate the new OCI Director's 90-day study and that Secretary Richardson did not assume his DOE duties until mid-August, but we find unacceptable the more than four months that

elapsed before DOE advised the National Security Advisor on the actions taken and specific remedies developed to implement the Presidential directive, particularly one so crucial.

More critically, we are disturbed by bureaucratic foot-dragging and even recalcitrance that ensued after issuance of the Presidential Decision Directive. Severe disagreements erupted over several issues, including whether the CI program would apply to all of the labs, and not just the weapons labs and the extent to which polygraph examinations would be used in the personnel security program. We understand that some DOE officials declined to assist in the implementation simply by declaring that, "It won't work." The polygraph program was finally accepted into the DOE's security reforms only after the National Security Advisor and the DCI personally interceded. The fact that the Secretary's implementation plan was not issued to the labs until more than a year after the PDD was issued tells us DOE is still unconvinced of Presidential authority. We find worrisome the reports of repeated and recent resistance by Office of Management and Budget (OMB) officials toward requests for funding to implement the counterintelligence reforms mandated by PDD-61. We find vexing the reports we heard of OMB budgeters lecturing other government officials on the "unimportance" of counterintelligence at DOE.

Secretary Richardson's Initiatives

Since November 1998 and especially since April of this year, Secretary Richardson has taken commendable steps to address DOE's security and counterintelligence deficiencies. In November 2000, in the action plan required by PDD-61, Secretary Richardson detailed 31 actions to be taken to reform DOE's counterintelligence program. These actions addressed the structure of the counterintelligence program, selection and training of field counterintelligence personnel, counterintelligence analysis, counterintelligence and security awareness, protections against potential "insider threats," computer security, and

relationships with the FBI, the Central Intelligence Agency, and the National Security Agency.

Though many matters addressed in the action plan would require further evaluation before specific actions would be taken, immediate steps included granting to the OCI direct responsibility for programming and funding counterintelligence activities of all DOE field offices and laboratories, granting the Director OCI the sole authority to propose candidates to serve as the counterintelligence officers at the weapons labs, and instituting a policy for a polygraph program for employees with access to sensitive information.

In April 1999, in an effort to eliminate multiple reporting channels and to improve lines of communications, direction, and accountability, Secretary Richardson ordered changes in the Department's management structure. In short, each of the 11 field offices reports to a Lead Program Secretarial Office (LPSO). The LPSO has "overall line accountability for site-wide environment, safety and health, for safeguards and security and for the implementation of policy promulgated by headquarters staff and support functions." A newly established Field Management Council is to be charged with program integration.

In May 1999, Secretary Richardson announced substantial restructuring of the security apparatus at DOE. Among these is the new Office of Security and Emergency Operations, which will report directly to the Secretary. It consists of the Office of the Chief Information Officer, the Office of Emergency Management and Response, and the Office of Security Affairs, which will include the Office of Safeguards and Security, the Office of Nuclear and National Security Information, the Office of Foreign Visits and Assignments, and the Office of Plutonium, Uranium, and Special Material Inventory. This office is responsible for all safeguards and security policy, cybersecurity, and emergency functions throughout DOE.

Also announced was the creation of the Office of Independent Oversight and Performance Assurance. It also will report directly to the

Secretary to provide independent oversight for safeguards and security, special nuclear materials accountability, and other related areas.

To support additional cyber-security improvements, DOE will be asking Congress for an additional \$50 million over the next two years. Improvements are to include continual monitoring of DOE computers for unauthorized and improper use. Also, new controls will be placed on computers and workstations, removable media, removable drives, and other devices that could be used to download files. In addition, warning "banners" are now mandatory on all computer systems to alert users that these systems are subject to search and review at the government's discretion. Cybersecurity training is also to be improved.

Secretary Richardson further announced additional measures designed to strengthen DOE's counterintelligence program. They include a requirement that DOE officials responsible for maintaining personnel security clearances be notified of any information that might affect the issuance or maintenance of such a clearance, even when the information does not rise to the level of a criminal charge; and mandatory reporting by all DOE employees of any substantive contact with foreign nationals from sensitive countries. DOE also plans to strengthen its Security Management Board; accelerate actions necessary to correct deficiencies in security identified in the 1997/1998 Annual Report to the President on Safeguards and Security; expedite improvements in the physical security of DOE nuclear weapons sites; and delay the automatic declassification of documents more than 25 years old.

In sum, as of mid-June 1999, progress has been made in addressing counterintelligence and security. Of note, all of the PDD-61 requirements are reported to have been substantially implemented. Other important steps also reportedly have been completed. Among these are the assignment of experienced counterintelligence officers to the weapons labs.

Prospects for Reforms

Although we applaud Secretary Richardson's initiative, we seriously doubt that his initiatives will achieve lasting success. Though certainly significant steps in the right direction, Secretary Richardson's initiatives have not yet solved the many problems. Significant objectives, all of which were identified in the DOE OCI study completed nearly a year ago, have not yet been fully achieved. Among these unmet objectives are revising the DOE policy on foreign visits and establishing an effective polygraph examination program for selected, high-risk programs. Moreover, the Richardson initiatives simply do not go far enough.

These moves have not yet accomplished some of the smallest fixes despite huge levels of attention and Secretarial priority. Consider the following example: with all the emphasis of late on computer security, including a weeks-long standdown of the weapons labs computer systems directed by the Secretary, the stark fact remains that, as of the date of this report, a nefarious employee can still download secret nuclear weapons information to a tape, put it in his or her pocket, and walk out the door. Money cannot really be the issue. The annual DOE budget is already \$18 billion. There must be some other reason.

Under the Richardson plan, even if the new "Security Czar" is given complete authority over the more than \$800 million ostensibly allocated each year to security of nuclear weapons-related functions in DOE, he will still have to cross borders into other people's fiefdoms, causing certain turmoil and infighting. If he gets no direct budget authority, he will be left with little more than policy guidance. Even then, as the head of a staff office under the most recent Secretary Richardson reorganization, he has to get the approval of yet another fiefdom, the newly created Field Management Council, before he can issue policy guidance. Moreover, he is unlikely to have much success in obtaining approval from that body when he is not even a member, and the majority of those

who are members are the very program managers that his policy guidance would affect.

Trouble Ahead

Perhaps the most troubling aspect of the PFIAB's inquiry is the evidence that the lab bureaucracies—after months at the epicenter of an espionage scandal with serious implications for US foreign policy—are still resisting reforms. Equally disconcerting, other agencies have joined the security skeptics' list. In the past few weeks, officials from DOE and other agencies have reported to the Rudman panel:

- There is a heightened attention to security at the most senior levels of DOE and the labs, but at the midlevel tiers of management there has been lackluster response and "business as usual."
- Unclassified but sensitive computer networks at several weapons labs are still riddled with vulnerabilities.
- Buildings that do not meet DOE security standards are still being used for open storage of weapons parts.
- Foreign nationals—some from sensitive countries—residing outside a weapons lab have remote dial-up access to unclassified networks without any monitoring by the lab.
- In an area of a weapons lab frequented by foreign nationals, a safe containing restricted data was found unsecured. Guards had not checked the safe since August 1998. When confronted with the violation, a midlevel official is said to have implied that it was not an actual security lapse because the lock had to be "jiggled" to open the safe door.
- A weapons lab was instructed to monitor its outgoing e-mail for possible security lapses. The lab took the minimal action necessary; it began monitoring e-mails but did not monitor the files attached to e-mails.
- When Secretary Richardson ordered the recent computer stand down, there was great resistance, and when it came time to decide if the labs' computers could be turned on again, a bevy of DOE officials fought to have final approval power.

Security and Counterintelligence Accountability

The agency director should issue clear guidelines on security accountability. The agency security chief must be accountable to the agency director for security policy at the labs, and the lab directors must be accountable to the agency director for compliance. The same system and process should be established to instill accountability among counterintelligence officials.

Attentive, independent oversight will be critical to ensuring high standards of security and counterintelligence performance at the new agency. In that regard, we welcome Senator John Warner's recent legislative initiative to create a small, dedicated panel to oversee security and counterintelligence performance at the weapons labs. This oversight should include an annual certification process.

Personnel Security

An Effective Personnel Security Program. The agency director should immediately undertake a total revamping of the "Q" clearance program and look to the security elements in the Intelligence Community for advice and support. This review should result in a complete rewrite of existing guidance and standards for the issuing, revoking, and suspending of security clearances. Special attention should be paid to establishing a clear—and relatively low—threshold for suspending clearances for cause, including pending criminal investigations.

The review also should significantly strengthen the background investigation process by restructuring contracts to create incentives for thoroughness. We strongly advocate abolishing the prevalent method of paying investigators "by the case." Strict "need-to-have" regulations should be issued for regular reviews of clearance requirements for all contract employees. Those without a continuing need should have their clearances withdrawn. The National Security Council should review and resolve issues on a government-wide basis that

permit a person who is under FBI investigation for suspected espionage to obtain a new or renewed clearance; existing standards for clearance renewal also should be reviewed with an eye toward tightening up.

A Professional Administrative Inquiry Process.

The agency Director should promulgate new agency guidelines and standards for security-related administrative inquiries to ensure that proper security/counterintelligence procedures and methods are employed. Very high professional qualification standards should be established and strictly maintained for all security personnel involved in administrative inquiries.

Physical/Technical/Cyber Security

Comprehensive Weapons Lab Cybersecurity Program. Under the sponsorship and specific guidance of the agency Director, the weapons labs should institute a broad and detailed program to protect all computer workstations, networks, links, and related systems from all forms of potential compromise. This program, which should be reviewed by and coordinated with appropriate offices within the US Intelligence Community, must include standard network monitoring tools and uniform configuration management practices. All lab computers and networks must be constantly monitored and inspected for possible compromise, preferably by an agency-sponsored, independent auditing body. The appropriate agency security authority should conduct on a yearly basis a "best practices" review.

Comprehensive Classified Document Control System. Document controls for the most sensitive data of the weapons labs should be re-instituted by the agency Director. The program should be constantly monitored by a centralized agency authority to ensure compliance.

Comprehensive Classification Review. The new agency, in coordination with the Intelligence Community, should promulgate new, concise, and precise classification guidance to define and ensure awareness of information and technologies

that require protection. This guidance should clear up the widespread confusion over what is export-controlled information; what information, when joined with other data, becomes classified; and the differences between similarly named and seemingly boundless categories such as “unclassified controlled nuclear information” and “sensitive but unclassified nuclear information.”

Business Issues

Make Security an Integral Part of Doing Business. Security compliance must be a major requirement in every agency contract with the weapons labs. Rather than a detailed list of tasks, the contract should make clear the security and counterintelligence standards by which the lab will be held accountable. It is the responsibility of the lab to develop the means to achieve those objectives. If a lab fails to conform to these standards and requirements, the agency should withhold performance award fees.

Review the Process for Lab Management Contracts. If the agency director has reason to open the bidding for lab management contracts, we strongly recommend an intensive market research effort. Such an effort would help ensure that legitimate and competent bidders, with strong records for productive research and development, participate in the competition.

Weapons Labs Foreign Visitors Program. This productive program should continue, but both the agency and the weapons labs, in concert, must ensure that secret information is protected. This means precise policy standards promulgated by the agency to ensure: the integrity of the secure areas and control over all foreign visitors and assignees, a clear demarcation between secure and open areas at the labs, strong enforcement of restrictions against sensitive foreign visitors and assignees having access to secure facilities, and sensible but firm guidelines for weapons lab employees’ contacts with foreign visitors from sensitive countries. Exceptions should be made by the agency director on a case-by-case basis. Clear, detailed standards should be enforced to determine

whether foreign visits and appointments receive approval. The burden of proof should be placed on the employees who propose to host visitors from sensitive countries. Visits should be monitored by the labs and audited by an independent office. The bottom line: treat foreign visitors and assignees with the utmost courtesy, but assume they may well be collecting information for other governments.

Foreign Travel Notification. The agency should institute a program whereby all agency and weapons lab employees in designated sensitive positions must make written notification of official and personal foreign travel well before departure. The agency must keep close records of these notifications and also ensure that effective counterintelligence briefings are provided to all such travelers. Unless formally granted an exception, scientists for weapons labs should travel in pairs on official visits to sensitive countries.

Counterintelligence. The FBI should explore the possibility of expanding foreign counterintelligence resources in its field offices near the weapons labs.

Intelligence Community Damage Assessment of China’s Acquisition of US Nuclear Weapons Information

Chinese strategic nuclear efforts have focused on developing and deploying a survivable long-range missile force that can hold a significant portion of the US and Russian populations at risk in a retaliatory strike. By at least the late 1970s, the Chinese launched an ambitious collection program focused on the United States, including its national laboratories, to acquire nuclear weapons technologies. By the 1980s, China recognized that its second strike capability might be in jeopardy unless its force became more survivable. This probably prompted the Chinese to heighten their interest in smaller and lighter nuclear weapon systems to permit a mobile force.

China obtained by espionage classified US nuclear weapons information that probably accelerated its program to develop future nuclear weapons. This collection program allowed China to focus

successfully down critical paths and avoid less promising approaches to nuclear weapons designs.

- China obtained at least basic design information on several modern US nuclear reentry vehicles, including the Trident II (W-88).
- China also obtained information on a variety of US weapon design concepts and weaponization features, including those of a neutron bomb.
- We cannot determine the full extent of weapon information obtained. For example, we do not know whether any weapon design documentation or blueprints were acquired.
- We believe it is more likely that the Chinese used US design information to inform their own program than to replicate US weapon designs.

China's technical advances have been made on the basis of classified and unclassified information deriving from espionage, contact with US and other countries' scientists, conferences and publications, unauthorized media enclosures, declassified US weapons information, and Chinese indigenous development. The relative contribution of each cannot be determined.

Regardless of the source of the weapons information, it has made an important contribution to the Chinese objective to maintain a second strike capability, and it has provided useful information for future designs.

Significant deficiencies remain in the Chinese weapons program. The Chinese almost certainly are using aggressive collection efforts to address deficiencies as well as to obtain manufacturing and production capabilities from both nuclear and non-nuclear sources.

To date, the aggressive Chinese collection effort has not resulted in any apparent modernization of their deployed strategic force or any new nuclear weapons deployment.

China has had the technical capability to develop a multiple independently targetable reentry vehicle (MIRV) system for its large, currently deployed ICBM for many years but has not done so. US information acquired by the Chinese could help them develop a MIRV for a future mobile missile.

We do not know if US classified nuclear information acquired by the Chinese has been passed to other countries. Having obtained more modern US nuclear technology, the Chinese might be less concerned about having their older technology.

Endnotes

¹ The Department of Energy National Weapons Labs and Plants discussed in this report are Lawrence Livermore National Lab, California; Los Alamos National Lab, New Mexico; Sandia National Lab, New Mexico; PANTEX Plant, Texas; Kansas City Plant, Missouri; Oak Ridge (Y-12) Plant, Tennessee.

² US Nuclear Command and Control System Support Staff, "Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process," March 1998.

³ US Nuclear Command and Control System Support Staff, "Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process," March 1998.

⁴ Classified DOE report.

⁵ Classified DOE report.

⁶ Classified DOE report.

⁷ Classified DOE report.

⁸ DOE, Office of Counterintelligence, "The Foreign Intelligence Threat to Department of Energy Personnel, Facilities and Research, Summary Report," August 1990.

⁹ Classified US Government report.

¹⁰ GAO/RCED-97-229, "Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," September 25, 1997.

¹¹ Hewlett, Richard G., and Francis Duncan, "Atomic Shield: A History of the U.S. Atomic Energy Commission," May 1969.

¹² Classified DOE report.

¹³ DOE, "Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security," February 1993

¹⁴ Classified FBI report.

¹⁵ Classified US Government report.

¹⁶ Classified DOE report.

¹⁷ DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1993," January 1994 (U).

¹⁸ DOE/IG-385, "Special Audit Report on the Department of Energy's Arms and Military-Type Equipment," 1 February 1996.

¹⁹ Classified DOE report.

²⁰ DOE, "Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities," September 1996.

²¹ GAO/RCED-91-12, "Nuclear Safety: Potential Security Weaknesses at Los Alamos and other DOE Facilities," October 1990 (U), and GAO/RCED-92-39, "Nuclear Security: Safeguards and Security Weaknesses

at DOE's Weapons Facilities," 13 December 1991.

²² GAO/RCED-90-122, "Nuclear Security: DOE Oversight of Livermore's Property Management System is Inadequate," 18 April 1990.

²³ GAO/"Key Factors Underlying Security Problems at DOE Facilities" (Statement of Victor S. Rezendes, Director, Energy, Resources and Science Issues, Resources, Community, and Economic Development Division, GAO, in testimony before the Subcommittee on Oversight and Investigations, Committee on Commerce, House of Representatives), 20 April 1999.

²⁴ Ibid.

²⁵ Classified DOE report.

²⁶ Hewlett, Richard G. and Francis Duncan, "Atomic Shield, A History of the United States Atomic Energy Commission," May 1969.

²⁷ GAO/RCED-89-34, "Nuclear Security: DOE Actions to Improve the Personnel Clearance Program," 9 November 1988.

²⁸ DOE/IG/WR-0-90-02, "Nevada Operations Office Oversight of Management and operating Contractor Security Clearances," March 1990.

²⁹ Classified DOE report.

³⁰ DOE/IG/WR-B-91-08, "Review of Contractor's Personnel Security Clearances at DOE Field Office, Albuquerque," September 1991.

³¹ DOE, "Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security," February 1993.

³² DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1995," January 1996.

³³ Classified US Government report.

³⁴ Classified DOE report.

³⁵ GAO/RCED-92-39, "Nuclear Security: Safeguards and Security Weaknesses at DOE Weapons Facilities," 13 December 1991.

³⁶ Classified DOE report.

³⁷ Classified DOE report.

³⁸ DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1993," January 1994. (U)

³⁹ DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1994," January 1995. (U)

⁴⁰ Classified DOE report.

⁴¹ Classified DOE report.

⁴² Classified DOE report.

⁴³ Classified DOE report.

⁴⁴ Classified DOE report.

⁴⁵ GAO/RCED-89-31, "Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories," 11 October 1988.

⁴⁶ Classified US Government report.

⁴⁷ GAO/RCED-97-229, "Department of Energy: DOE Needs To Improve Controls Over Foreign Visitors to Weapons Laboratories," 25 September 1997.

⁴⁸ Classified DOE report.

⁴⁹ GAO/RCED-97-229, "Department of Energy: DOE Needs To Improve Controls Over Foreign Visitors to Weapons Laboratories," 25 September 1997.

⁵⁰ Ibid.

⁵¹ DOE, "Response to the Cox Committee Report: The Benefits of Department of Energy International Scientific and Technical Exchange Programs," April 1999.

⁵² GAO/RCED-99-19, "Department of Energy: Problems in DOE's Foreign Visitors Program Persist," 6 October 1998.

⁵³ In April 1997, the FBI Director met with Secretary Pena, who had taken office in March, to deliver a highly critical FBI assessment of DOE's counterintelligence program. In June, DOE officials briefed the Special Assistant to the President and Senior Director for Nonproliferation and Export Controls. In July, the FBI Director and the Director of Central Intelligence expressed serious concern that DOE had not moved to implement the recommendations in the FBI report.

⁵⁴ The National Counterintelligence Policy Board (NACIPB) was created by a 1994 Presidential Decision Directive to serve as the National Security Council's primary mechanism to develop an effective national counterintelligence program. Current core NACIPB members include senior representatives from the Director of Central Intelligence/Central Intelligence Agency, the Federal Bureau of Investigation, the Department of Defense, the Department of State, the Department of Justice, the military departments' CI organizations, the National Security Council, and, as of 1997, the Department of Energy and NSA.

Central Intelligence Agency Inspector General

REPORT OF INVESTIGATION

IMPROPER HANDLING OF CLASSIFIED INFORMATION BY JOHN M. DEUTCH (1998-0028-IG)

February 18, 2000

L. Britt Snider
Inspector General

Daniel S. Seikaly
Assistant Inspector General for Investigations

This Report contains information that is or may be subject to the protections of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, or that otherwise may implicate the privacy interests of various current or former federal employees and private citizens.

This unclassified report has been prepared from the July 13, 1999 version of the classified Report of Investigation at the request of the Senate Select Committee on Intelligence. Information in this version is current as of the date of the original report. All classified information contained in the original Report of Investigation has been deleted.

INTRODUCTION

1. John M. Deutch held the position of Director of Central Intelligence (DCI) from May 10, 1995 until December 14, 1996. Several days after Deutch's official departure as DCI, classified material was discovered on Deutch's government-owned computer, located at his Bethesda, Maryland residence.
2. The computer had been designated for unclassified use only and was connected to a modem. This computer had been used to access [an Internet Service Provider (ISP)], the Internet, [Deutch's bank], and the Department of Defense (DoD). This report of investigation examines

Deutch's improper handling of classified information during his tenure as DCI and how CIA addressed this matter.

3. Currently, Deutch is a professor at the Massachusetts Institute of Technology. He also has two, no-fee contracts with the CIA. The first is to provide consulting services to the current DCI and his senior managers; this contract went into effect on December 16, 1996, has been renewed twice, and will expire in December 1999. The second contract is for Deutch's appointment to serve on the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (Proliferation Commission). Under the terms of the second contract, this appointment will continue until the termination of the Commission.

SUMMARY

4. The discovery of classified information on Deutch's unclassified computer on December 17, 1996 was immediately brought to the attention of senior Agency managers. In January 1997, the Office of Personnel Security (OPS), Special Investigations Branch (SIB), was asked to conduct a security investigation of this matter.¹ A technical exploitation team, consisting of personnel expert in data recovery, retrieved the data from Deutch's unclassified magnetic media and computers. The results of the inquiry were presented to CIA senior management in the spring and summer of 1997.
5. The Office of General Counsel (OGC) had been informed immediately of the discovery of classified information on Deutch's computer. Although such a discovery could be expected to generate a crimes report to the Department of Justice (DoJ), OGC determined such a report was not necessary in this case. No other actions, including notification of the Intelligence Oversight Committees of the Congress² or the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board, were taken until the Office of Inspector General (OIG)

opened a formal investigation in March 1998. On March 19, 1998, OIG referred the matter to DoJ. On April 14, 1999, the Attorney General declined prosecution and suggested a review to determine Deutch's suitability for continued access to classified information.

6. Deutch continuously processed classified information on government-owned desktop computers configured for unclassified use during his tenure as DCI. These unclassified computers were located in Deutch's Bethesda, Maryland and Belmont, Massachusetts residences,³ his offices in the Old Executive Office Building (OEOB), and at CIA Headquarters. Deutch also used an Agency-issued unclassified laptop computer to process classified information. All were connected to or contained modems that allowed external connectivity to computer networks such as the Internet. Such computers are vulnerable to attacks by unauthorized persons. CIA personnel retrieved [classified] information from Deutch's unclassified computers and magnetic media related to covert action, Top Secret communications intelligence and the National Reconnaissance Program budget.
7. The OIG investigation has established that Deutch was aware of prohibitions relating to the use of unclassified computers for processing classified information. He was further aware of specific vulnerabilities related to the use of unclassified computers that were connected to the Internet. Despite this knowledge, Deutch processed a large volume of highly classified information on these unclassified computers, taking no steps to restrict unauthorized access to the information and thereby placing national security information at risk.
8. Furthermore, the OIG investigation noted anomalies in the way senior CIA officials responded to this matter. These anomalies include the failure to allow a formal interview of Deutch, and the absence of an appropriate process to review Deutch's suitability for continued access to classified information.

BACKGROUND

9. In 1998, during the course of an unrelated investigation, OIG became aware of additional circumstances surrounding an earlier allegation that in 1996 Deutch had mishandled classified information. According to the 1996 allegation, classified information was found on a computer configured for unclassified use at Deutch's Maryland residence. This computer had been used to connect to the Internet. Additionally, unsecured classified magnetic media was found in Deutch's study at the residence. Further investigation uncovered additional classified information on other Agency-owned unclassified computers issued to Deutch. In 1998, OIG learned that senior Agency officials were apprised of the results of the OPS investigation but did not take action to properly resolve this matter. The Inspector General initiated an independent investigation of Deutch's alleged mishandling of classified information and whether the matter was appropriately dealt with by senior Agency officials.

PROCEDURES AND RESOURCES

10. OIG assigned a Supervisory Investigator, five Special Investigators, a Research Assistant, and a Secretary to this investigation. The team of investigators interviewed more than 45 persons thought to possess knowledge pertinent to the investigation, including Deutch, DCI George Tenet, former CIA Executive Director Nora Slatkin, former CIA General Counsel Michael O'Neil, and [the] former FBI General Counsel. The team reviewed security files, memoranda for the record written contemporaneously with the events under investigation, data recovered from Deutch's unclassified magnetic media, Congressional testimony, and material related to cases involving other individuals who mishandled classified information. Pertinent information was also sought from the National Security Agency (NSA), the DoD, and an Internet service provider (ISP). In addition, the team reviewed applicable criminal statutes,

Director of Central Intelligence Directives, and Agency rules and regulations.

QUESTIONS PRESENTED

11. This Report of Investigation addresses the following questions:

- Why was Deutch issued government computers configured for unclassified use and were his computer systems appropriately marked as unclassified?
- Why was Deutch permitted to retain government computers after resigning as DCI?
- What information was found on Deutch's magnetic media?
 - How was the classified material discovered?
 - What steps were taken to gather the material?
 - What steps were taken to recover information residing on Deutch's magnetic media?
 - What are some examples of the classified material that was found?
- What vulnerabilities may have allowed the hostile exploitation of Deutch's unprotected computer media?
 - What was the electronic vulnerability of Deutch's magnetic media?
 - What was the physical vulnerability of Deutch's magnetic media?
- Could it be determined if classified information on Deutch's unclassified computer was compromised?
- What knowledge did Deutch have concerning vulnerabilities associated with computers?
 - What is Deutch's recollection?
 - What did Deutch learn at [an] operational briefing?
 - What was Deutch's Congressional testimony?
 - What are the personal recollections of DCI staff members?
- Had Deutch previously been found to mishandle classified information?
- What laws, regulations, agreements, and policies have potential application?
- How was a similar case handled?
- What actions did senior Agency officials take in handling the Deutch case?
 - What actions were taken by senior Agency

officials after learning of this matter?	December 13	Deutch signs a no-fee-consulting contract permitting him to retain government computers.
<ul style="list-style-type: none"> • How were the Maryland Personal Computer Memory Card International Association (PCMCIA) cards handled? • What was the course of the Special Investigations Branch's investigation of Deutch? • Should a crimes report initially have been filed on Deutch in this case? • Should application of the Independent Counsel statute have been considered? • Were senior Agency officials obligated to notify the Congressional oversight committees or the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board? Were these entities notified? • Why was no administrative sanction imposed on Deutch? • What was OIG's involvement in this case? <ul style="list-style-type: none"> • When did OIG first learn of this incident? • Why did OIG wait until March 1998 to open an investigation? • What steps were taken by OIG after opening its investigation? • What is Deutch's current status with the CIA? • What was the disposition of OIG's crimes report to the Department of Justice? 	December 14	Deutch's last day as DCI.
	December 17	Classified information found on Deutch's computer in Bethesda, Maryland. Slatkin and O'Neil notified. Slatkin notifies Tenet within a day. O'Neil informs Deutch of discovery.
	December 23	Four PCMCIA cards retrieved from Deutch and given to O'Neil.
	December 27	Hard drive from Deutch's Maryland computer retrieved.
	December 28	Chief/DCI Administration informs IG Hitz of discovery at Deutch's residence.
	December 30	Hard drives from residences given to O'Neil.
1997		

CHRONOLOGY OF SIGNIFICANT EVENTS

1995

January 1	John Deutch establishes Internet access via an [ISP provider].
May 10	Deutch sworn in as DCI.
June 15	Earliest classified document later recovered by technical exploitation team.
August 1	Deutch receives [a] briefing on computer attacks.

1996

December 5	Deutch requests that he be able to retain computers after he leaves office.
------------	-----------------------------------------------------------------------------

January 6	OPS/SIB initiates investigation on Deutch. PDGC and the OPS Legal Advisor discuss issue of a crimes report.
January 9	O'Neil releases to DDA Calder and C/SIB the hard drives from the residences and two of six PCMCIA cards. O'Neil retains four PCMCIA cards from the Maryland residence.
January 9	Memo from ADCI to D/OPS directing Deutch to keep clearances through December 1997.
January 13	Technical exploitation team begins the recovery process.

January 22 Technical exploitation team documents that two hard drives contain classified information and had Internet exposure after classified material placed on drives.

January 30 O'Neil speaks with FBI General Counsel and was reportedly told that FBI was not inclined to investigate.

February 3 O'Neil releases four remaining PCMCIA cards that are subsequently exploited.

February 21 C/SIB meets with OIG officials to discuss jurisdictional issues.

February 27 D/OPS tasked to review all material on hard drives and PCMCIA cards.

March 11 D/OPS completes review of 17,000 pages of recovered items.

July 8 D/OPS's report to ADCI prepared for distribution. Included on distribution are Slatkin, O'Neil, and Richard Calder.

July 21 Slatkin is replaced as Executive Director.

July 30 PDGC reaffirms with OGC attorney that original disks and hard drives need to be destroyed to ensure protection of Deutch's privacy.

August 11 PDGC appointed Acting General Counsel and O'Neil goes on extended annual leave.

August 12 Technical exploitation team confirms selected magnetic media were destroyed per instruction of D/OPS.

September 8 Slatkin leaves CIA.

October 1 O'Neil retires from CIA.

November 24 DCI approves Deutch and other members of the Proliferation Commission for temporary staff-like access to CIA information and facilities without polygraph.

1998

February 6 OIG is made aware of additional details of the SIB investigation and subsequently opens a formal investigation.

March 19 IG forwards crimes report to DoJ.

May 8 IG letter to IOB concerning Deutch investigation.

June 2 DCI notifies oversight committees of investigation.

1999

April 14 Attorney General Reno declines prosecution and suggests a review of Deutch's security clearances.

FINDINGS

WHY WAS DEUTCH ISSUED GOVERNMENT COMPUTERS CONFIGURED FOR UNCLASSIFIED USE AND WERE HIS COMPUTER SYSTEMS APPROPRIATELY MARKED AS UNCLASSIFIED?

12. The then-Chief of the Information Services Management Staff (C/ISMS) for the DCI Area, recalled that prior to Deutch's confirmation as DCI, she was contacted by [Deutch's Executive Assistant] regarding computer requirements for Deutch. C/ISMS, who would subsequently interface with [the Executive Assistant] on a routine basis, learned that

Deutch worked exclusively on Macintosh computers. An Information Security (Infosec) Officer assigned to ISMS recalled C/ISMS stating that [the Executive Assistant] instructed [her] to provide Internet service at the 7th floor Headquarters suite, OEOB, and Deutch's Maryland residence.

13. According to C/ISMS, Deutch's requirements, as imparted by [his Executive Assistant], were for Deutch to have not only access to the Internet, including electronic messaging, but access to CIA's classified computer network from Deutch's offices in CIA Headquarters, OEOB, and his Maryland residence. In addition, Deutch was to be issued an unclassified laptop with Internet capability for use when traveling.
14. A computer specialist, who had provided computer support to Deutch at the Office of the Secretary of Defense, confirmed that, at Deutch's request, he had been hired by CIA to establish the same level of computer support Deutch had received at the Pentagon. At CIA, the computer specialist provided regular and close computer support to Deutch on an average of once a week. The computer specialist recalled [that Deutch's Executive Assistant] relayed that he and Deutch had discussed the issue of installing the classified computer at Deutch's Maryland residence, and Deutch either did not believe he needed or was not comfortable having the classified computer in his home.
15. [Deutch's Executive Assistant] also remembered discussions about locating a classified computer at Deutch's Maryland residence. [The Executive Assistant], however, could not recall with any certainty if the computer had in fact been installed. [The Executive Assistant] said that a classified system had been installed at his own residence. However, after using it once, he found its operation to be difficult and time consuming, and he had it removed from his residence. [The Executive Assistant's] experience with

the deployed classified system may have influenced Deutch to decide he did not want one located at his Maryland residence. If so, [the Executive Assistant] would have informed the ISMS representative of Deutch's decision.

16. C/ISMS recalled [the Executive Assistant] telling her he was not sure Deutch required a classified computer system at Deutch's Maryland residence.
17. A Local Area Network (LAN) technician installed classified and unclassified Macintosh computers in Deutch's 7th floor Headquarters office and in Deutch's OEOB office. The technician also installed a computer configured for unclassified use at Deutch's Maryland residence. The technician stated that Deutch was also provided with an unclassified laptop that had an internal hard drive with modem and Internet access. The computer specialist installed an unclassified computer at Deutch's Belmont residence several months after Deutch was appointed DCI.
18. Personal Computer Memory Card International Association (PCMCIA) cards are magnetic media capable of storing large amounts of data. According to the computer specialist, Deutch's unclassified computers were equipped with PCMCIA card readers. The computer specialist said this configuration afforded Deutch the opportunity to write to the cards and back up information. One PCMCIA card would reside at all times in a reader that was attached to the unclassified computer, and the other PCMCIA card would be in Deutch's possession. The computer specialist stated that Deutch valued the ability to access, at several locations, data on which he was working. C/ISMS stated that all the unclassified computers and PCMCIA cards provided for Deutch's use contained a green label indicating the equipment was for unclassified purposes. The LAN technician also stated that a concern was to label all of Deutch's automated data processing equipment and magnetic media, including

monitors and PCMCIA cards, as either “unclassified” (green label) or “Top Secret” (purple label). The technician stated that his purpose was to make it perfectly clear to Deutch and anyone else using these systems, what was for classified and unclassified use.

19. The OIG has in its possession eight PCMCIA cards that had been used by Deutch. Seven of the eight cards were labeled unclassified; the eighth was not labeled. Four of the cards were from the Maryland residence. Three of the cards were from CIA Headquarters and one was from the OEOP. In addition, OIG received four Macintosh computers and one Macintosh laptop that were used by Deutch. The laptop and two of the computers were marked with green unclassified labels; the other two computers were marked with purple classified labels. One of the classified computers was determined to have come from Deutch’s 7th floor Headquarters office; the other from his OEOP office.

WHY WAS DEUTCH PERMITTED TO RETAIN GOVERNMENT COMPUTERS AFTER RESIGNING AS DCI?

20. In a Memorandum for the Record (MFR) dated December 30, 1996, [the] then Chief DCI Administration (C/DCI Administration), noted that Deutch announced on December 5, 1996 that he would resign as DCI. That same day, according to C/DCI Administration’s MFR, Deutch summoned [him] to his office. Deutch told [him] “to look at a way in which he could keep his government computers.”
21. The C/DCI Administration’s MFR indicated that on December 6, 1996, he spoke with [the then] Chief of the Administrative Law Division⁴ (C/ALD) in OGC, to ask if Deutch could retain his Agency-issued, unclassified computer after leaving CIA. C/ALD reportedly said that he had concerns with government-owned property that was to be utilized for personal use. He advised that he would discuss the matter with the Principal Deputy General Counsel (PDGC).

22. On December 9, 1996, C/DCI Administration asked ISMS personnel to identify a system configuration which was identical to Deutch’s. [He] hoped that Deutch would purchase a computer instead of retaining a government-owned computer.

23. According to a December 19, 1996 MFR signed by C/ALD and the PDGC, [C/ALD] discussed with [her] the request to loan computers to Deutch.⁵ [She] mentioned the request to General Counsel Michael O’Neil, and stated:

The only legal way to loan the computers to the DCI would be if a contract was signed setting forth that John Deutch was a consultant to the CIA, and that the computers were being loaned to Mr. Deutch to be used solely for U.S. Government business.

24. Despite her reservations, the PDGC was told by O’Neil to work with C/DCI Administration to formulate a contract for Deutch to be an unpaid consultant. The contract would authorize the provision of a laptop computer for three months and a desktop computer for up to a year.

25. According to the MFR:

On or about 11 December, [the PDGC] was informed by [C/DCI Administration] that the DO wanted the computers loaned to him because they had the DO’s personal financial data on them and he wanted access to that data. [C/DCI Administration] learned this information in conversation with the DCI. [The PDGC] informed [C/ALD] of this development, and they both agreed that it was improper to loan the computers to the DCI if the true purpose of the loan was to allow the DCI to have continued access to his personal information. [The PDGC] and [C/ALD] also expressed concern that the computers should not have been used by the DCI to store personal financial records since this would constitute improper use of a government computer. [C/

ALD] held further conversations with [C/DCI Administration] at which time [C/ALD] suggested that the DCI's personal financial data be transferred to the DCI's personal computer rather than loaning Agency computers to the DCI. [C/DCI Administration] stated that this proposal would not work because the DCI did not own any personal computers. It was then suggested that the DCI be encouraged to purchase a personal computer and that the DCI personal financial records be transferred to the computer.

26. On December 10, 1996, a no-fee contract was prepared between John Deutch, Independent Contractor, and the CIA. Deutch was to provide consulting services to the DCI and senior managers, was to retain an Agency-issued laptop computer for three months, and would retain an Agency-issued desktop computer for official use for one year.

27. C/DCI Administration's MFR notes that on December 13, 1996, he spoke with O'Neil on the telephone. O'Neil directed that the contract being prepared for Deutch be modified to authorize Deutch two computers for a period of one year. The contract was revised on December 13, 1996; the reference to the laptop was deleted but Deutch was to retain two Agency-issued desktop computers and two STU-III secure telephones for one year.

28. According to the C/DCI Administration's MFR, on December 12, 1996, [he] again met with Deutch to discuss matters relating to Deutch's departure. The computer issue was again discussed:

I mentioned again that I had "strong reservations" about Mr. Deutch maintaining the Government-owned computers and restated that we would be happy to assist moving Mr. Deutch to a personally-owned platform. Mr. Deutch slammed shut his pen drawer on his desk and said thanks for everything without addressing the issue.

29. According to the C/ALD and PDGC MFR, they met with O'Neil on December 13, 1996 to discuss the loan of the computers to Deutch. [They] expressed concern that the loan of the computers would be improper if Deutch intended to use the computers for personal purposes. O'Neil stated that he had discussed the matter with Deutch, and Deutch knew he could not use the computers for personal purposes. O'Neil also stated, according to the MFR, that Deutch had his own personal computers and that Deutch would transfer any personal data from the CIA computers to his own. O'Neil said that the contract, which only called for the loan of two computers, had to be re-drafted so that it would cover the loan of a third computer. O'Neil advised that Deutch would not agree to an arrangement in which he would simply use his own computers for official work in place of a loaned CIA computer.⁶

30. The PDGC recalls standing in the receiving line at a farewell function for Deutch and being told by Deutch's wife, "I can't believe you expect us to go out and buy another computer."

31. The MFR indicates that [the two OGC attorneys] dropped their objections to the loan of the computers, based on assurances from O'Neil that Deutch understood the computers would only be used for official purposes, and he would transfer his personal financial data to his own computer.

32. The contract was signed on December 13, 1996 by O'Neil and Deutch. The effective date for the contract was December 16, 1996. The contract states that Deutch "shall retain, for Government use only, two (2) Agency-issued desktop computers and two (2) STU-III's for the period of one year." Instead, Deutch was issued three PCMCIA cards and two PCMCIA card readers and all government-owned computers were returned to the Agency. On June 23, 1997, he purchased the cards and readers from CIA for \$1,476.

WHAT INFORMATION WAS FOUND ON DEUTCH'S MAGNETIC MEDIA?

How was the classified material discovered?

33. Each of the two, unclassified, Agency-owned computers that were to be loaned to Deutch under the provisions of the December 13, 1996 contract were already located at Deutch's Maryland and Belmont residences. To effect the loan of the computers, C/DCI Administration, after consulting with Deutch and his personal assistant, requested that an Infosec Officer perform an inventory of the two government-owned Macintosh computers and peripherals at the Deutch residences. In addition, the Infosec Officer was to do a review to ensure no classified material had been accidentally stored on these computers. While at the Deutch residences, a contract engineer was to document the software applications residing on the computers and, at Deutch's request, install several software applications. This software included FileMaker Pro (e.g., a database) that was to be used with a calendar function and Lotus Notes that would be used with an address book. Deutch has no recollection of authorizing an inventory or a personal visit to his residences and questions the appropriateness of such a visit.
34. On December 17, 1996, the contract network engineer and the Infosec Officer, escorted by a member of the DCI security protective staff, entered Deutch's Maryland residence to conduct the review of the unclassified Macintosh computer and its peripherals. The Infosec Officer reviewed selected data on the computer and two PCMCIA cards, labeled unclassified, located in each of two PCMCIA card drives. Two other PCMCIA cards, one labeled unclassified and the other not labeled, were located on Deutch's desk.
35. The Infosec Officer's initial review located six files containing what appeared to be sensitive

or classified information. Although the Infosec Officer believed that numerous other classified or sensitive files were residing on the computer, he concluded the system was now classified and halted his review. The contract network engineer agreed the system should be considered classified based on the information residing on the computer.

36. In addition to these six files, the contract network engineer and the Infosec Officer noted applications that allowed the Macintosh computer external connectivity via a FAX modem. The computer also had accessed the Internet via [an ISP], a DoD unclassified e-mail system, and [Deutch's bank] via its proprietary dial-up software.

What steps were taken to gather the material?

37. The Infosec Officer telephoned C/DCI Administration and informed him of the discovery of classified material. Although normal information security practice would have been to immediately confiscate the classified material and equipment, C/DCI Administration advised the Infosec Officer to await further instruction. [He] proceeded to contact then-CIA Executive Director Nora Slatkin. She referred him to O'Neil for guidance. [He] stated that he consulted with O'Neil, who "requested that we print off copies of the documents for his review." [He] contacted the Infosec Officer and instructed him to copy the six classified/sensitive files to a separate disk and return to Headquarters. The Infosec Officer copied five of the six files.⁷
38. After returning to Headquarters, the contract network engineer recalled being contacted by O'Neil. O'Neil advised that he had spoken with Deutch, and Deutch could not understand how classified information came to be found on the computer's hard drive. O'Neil wanted to know if any extraordinary measures were used to retrieve the classified documents

and was told the documents were simply opened using Microsoft Word. O'Neil asked the contract network engineer to wait while Deutch was again contacted.

39. Shortly thereafter, the contract engineer stated that Deutch telephoned him and said he could not understand how classified information could have been found on the computer's hard drive as he had stored such information on the PCMCIA cards. The contract engineer told Deutch that the classified information had been found on the PCMCIA cards. The contract engineer recalled suggesting that Deutch might want a new hard drive and replacement PCMCIA cards to store unclassified files that could be securely copied from Deutch's existing PCMCIA cards. According to the contract engineer, Deutch agreed but wanted to review the PCMCIA card files first because they contained personal information.
40. On December 23, 1996, Deutch provided the four PCMCIA cards from his Maryland residence to the DCI Security Staff. These four cards were delivered to O'Neil the same day.
41. On December 27, 1996, the contract network engineer advised C/DCI Administration that two PCMCIA cards previously used by Deutch had been located in an office at Headquarters. One of the cards had an unclassified sticker and was labeled as "Deutch's Personal Disk." The other did not have either a classification sticker or a label. The files on the card with the unclassified sticker had been erased; however, the contract network engineer was able to recover data by the use of a commercially available software utility. Although labeled "unclassified," the contract network engineer noted that the files contained words such as "Secret," "Top Secret Codeword," "CIA," and the name of an Office of Development and Engineering facility. This discovery caused C/DCI Administration, on the advice of [the] Associate Deputy

Director for Administration (ADDA),⁸ to contact O'Neil for assistance in expeditiously retrieving Deutch's Macintosh computers from the Maryland and Belmont residences.

42. On the evening of December 27, 1996, the contract network engineer visited Deutch's Maryland residence, removed Deutch's hard drive, and delivered it to C/DCI Administration. On December 30, 1996, DCI Security Staff delivered to C/DCI Administration the hard drive from Deutch's Belmont residence. Both hard drives were then delivered to O'Neil.
43. On January 6, 1997, OPS/SIB, upon the approval of Slatkin, initiated an internal investigation to determine the security implications of the mishandling of classified information by Deutch.
44. According to Slatkin, she, O'Neil, and Richard Calder, Deputy Director for Administration had several discussions about how to proceed with the investigation. She also discussed with Acting DCI Tenet the issue of how to proceed. As a result, a select group was created to address this matter. Its purpose was to (1) take custody of the magnetic media that had been used by Deutch, (2) review Deutch's unclassified magnetic media for classified data, (3) investigate whether and to what extent Deutch mishandled classified information, and (4) determine whether classified information on Deutch's computers that had Internet connectivity was compromised.
45. By January 13, 1997, all hardware and files that had been used by Deutch, except four PCMCIA cards retrieved from Deutch's Maryland residence on December 23, 1996, were in SIB's possession. On February 3, 1997, O'Neil released the four PCMCIA cards to Calder, who transferred them to the group on February 4, 1997. Then-Director of Personnel Security (D/OPS) headed the group. Calder was the senior focal point for

the group. In addition, a technical exploitation team was formed to exploit the magnetic media.

What steps were taken to recover information residing on Deutch's magnetic media?

46. Five government-issued MacIntosh computer hard drives and eight PCMCIA cards, used by Deutch and designated for unclassified purposes, were examined by a technical exploitation team within the group. Because each of the computers had modems, the PCMCIA cards were considered equally vulnerable when inserted into the card readers attached to the computers. The group had concerns that the processing of classified information on Deutch's five computers that were designated for unclassified information were vulnerable to hostile exploitation because of the modems. The group sought to determine what data resided on the magnetic media and whether CIA information had been compromised.
47. The examination of Deutch's magnetic media was conducted during the period January 10 through March 11, 1997. The technical exploitation team consisted of a Senior Scientist and two Technical Staff Officers, whose regular employment responsibilities concerned [data recovery]. The Infosec Officer who participated in the December 17, 1996 security inspection at Deutch's Maryland residence also assisted in the exploitation effort.
48. This team performed the technical exploitation of Deutch's magnetic media, recovered full and partial documents containing classified information, and printed the material for subsequent review. Technical exploitation began with scanning for viruses and making an exact copy of each piece of media used by Deutch. Further exploitation was performed on the copies. The original hard drives and PCMCIA cards were secured in safes. The copies were restored, in a read-only mode, on

computers used by the team. Commercially available utility software was used to locate, restore, and print recoverable text files that had been erased. In an attempt to be exhaustive, the Senior Scientist wrote a software program to organize text fragments that appeared to have been part of word processing documents.

49. To accommodate concerns for Deutch's privacy, D/OPS was selected to singularly review all recovered data. He reviewed in excess of 17,000 pages of recovered text to determine which documents should be retained for possible future use in matters relating to the unauthorized disclosure of classified information.
50. Three of the PCMCIA cards surrendered by Deutch subsequent to the security inspection of December 17, 1996, were found to have characteristics that affected exploitation efforts. Specifically, the card labeled "John Backup" could not be fully exploited as 67 percent of the data was unrecognizable due to "reading" errors. The card labeled "Deutch's Disk" was found to have 1,083 "items" that were erased. The last folder activity for this card occurred on "December 20, 1996 at 5:51 [p.m.]." The third card, labeled "Deutch's Backup Disk" and containing files observed during the security inspection, was found to have been reformatted.⁹ The card was last modified on "December 20, 1996, [at] 5:19 p.m."
51. Subsequent investigation by OIG revealed that Deutch had paged the contract network engineer at 1000 hours on Saturday, December 21, 1996. In an e-mail to C/DCI Administration the following day, the contract network engineer wrote:

... he [Deutch] was experiencing a problem deleting files from one or [sic] his 170MB PCMCIA disks. As near as I [Contractor] can tell the disk has become corrupted and while it appears to allow him [Deutch] to copy files it did not allow him to delete them. We tried several techniques to get around the problem

but none were successful. He [Deutch] indicated that he [Deutch] would continue to copy files and not worry about deleting any additional files. He [Deutch] asked what we were going to do with the disks he returned and I told him that we would in all probability degauss them and then physically destroy them....

maintained by Deutch while he served at the DoD and CIA.

52. The exploitation efforts resulted in eight pieces of magnetic media yielding classified information. Of the eight pieces, four computers and three PCMCIA cards had prominent markings indicating that the equipment was for unclassified use.¹⁰ Forty-two complete documents [were classified up to Top Secret and a non-CIA controlled compartmented program] and 32 text or document fragments classified up to [Top Secret and a non-CIA controlled compartmented program] were recovered. Fourteen of the recovered classified documents contained actual printed classification markings (i.e., “SECRET,” “Top Secret/ [a non-CIA controlled compartmented program]”) as part of the document. These documents were located on hard drives and/or PCMCIA cards linked to Deutch’s residences, 7th floor CIA office, and laptop.
53. Indications of Internet, [an ISP],¹¹ an unclassified Pentagon computer e-mail,¹² and online banking usage were found on several of the storage devices. A virus was found to have corrupted a file on the computer formerly located in Deutch’s 7th floor CIA office. This computer was labeled “DCI’s Internet Station Unclassified,” but yielded classified information during the exploitation effort.
54. Recovered computer-generated activity logs reflect, in certain instances, classified documents were created by “John Deutch” during the period of June 1, 1995 and November 14, 1996. Many of the same documents, in varying degrees of completion, were found on different pieces of magnetic media. Additionally, the team recovered journals (26 volumes) of daily activities
55. The following text box provides a summary of Deutch’s magnetic media that resulted in the recovery of classified information.

Media/Location	Markings	Connected To	Information Recovered
Quatum ProDrive Hard Drive/Deutch's Maryland Residence	"Unclassified" on MacIntosh Power PC	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Six complete classified documents and text fragments including TS/Codeword. Internet (ISP), (Deutch's bank), and DoD electronic mail usage. Indicators of visits to high risk Internet sites. ¹³
Microtech PCMCIA Card/Deutch's Maryland Residence	"Deutch's Disk," "Unclassified," GS001490	PCMCIA Card Reader Networked to U.S. Robotics Fax Modem	Three complete classified documents and text fragments including TS/Codeword. ¹⁴ (Bank) online usage. Card apparently reformatted on 12/20/96 at 5:51 p.m.
Microtech PCMCIA Card/Deutch's Maryland Residence	"Deutch's Backup Disk," "Unclassified," GS001490	PCMCIA Card Reader Networked to U.S. Robotics Fax Modem	31 complete classified documents and text fragments, five observed during security inspection. (Bank) Online Usage. Card apparently reformatted on 12/20/96 at 5:19 p.m.
Quatum ProDrive Hard Drive/Deutch's Belmont Residence	"JMD" on Drive Shell	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Six complete classified documents and text fragments including TS/Codeword. Internet usage. Indicators of visits to high risk Internet sites.
MacIntosh Power PC with Hard Drive/Deutch's 7th Floor Office, Original Headquarters Building	"Unclassified," "Property of O/DI. . ." "DCI's Internet Station" Unclassified	U.S. Robotics Fax Modem Two PCMCIA Card Readers	One complete classified document and text fragments including TS/Codeword. Word macro concept virus. Internet, DoD electronic mail usage.
MacIntosh Power PC with Hard Drive/Deutch's OEOB	"Unclassified," "Property of DCI. . ."	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Text fragments including TS/Codeword. DoD electronic mail usage.
MacIntosh Powerbook Laptop	"Dr. Deutch Primary" "Unclassified"	Global Village Internal Modem	Two complete classified documents and text fragments including TS/Codeword.
	"Property of DCI. . ."		
Microtech PCMCIA Card/ISMS Office	"Deutch's Personal Disk," "Unclassified"	N/A	Text fragments including TS/Codeword.

What are some examples of the classified material that was found?

56. An October 7, 1996 memorandum from Deutch to the President and the Vice President, found on the hard drive of the Maryland residence computer [contained information at the Top Secret/Codeword level]. The last paragraph of the memorandum notes [that the information is most sensitive and must not be compromised]:

Accordingly, with (National Security Advisor) Tony's [Lake] advice, I have restricted distribution of this information to Chris [Secretary of State Warren Christopher], Bill [Secretary of Defense William Perry], Tony [Lake], Sandy [Deputy National Security Advisor Sandy Berger], Leon Fuerth [the VP's National Security Advisor], and Louie Freeh with whom I remain in close touch.

57. [The] former Chief of Staff to the DCI and Slatkin both identified the memorandum as one Deutch composed on the computer at his Maryland residence in their presence on October 5, 1996.
58. In a memorandum to the President that was found on a PCMCIA card from the Maryland residence, Deutch described an official trip. [The memorandum discussed information classified at the Top Secret level.]
59. In a memorandum to the President, which was found on a PCMCIA card from the Maryland residence, concerning a trip Deutch [discusses information classified at the Top Secret/Codeword level].
60. Deutch's memorandum to the President found on a PCMCIA card from the Maryland residence also [discusses a non-CIA controlled compartmented program].
61. An undated memorandum from Deutch to the President that was found on a PCMCIA card from the Maryland residence discusses a

trip. [The memorandum discusses information classified at the Secret level.]

62. Another Deutch memorandum to the President that was found on a PCMCIA card from the Maryland residence [discusses information classified at the Secret/Codeword level].
63. In a memorandum to the President that was found on a PCMCIA card from the Maryland residence, Deutch [discusses information classified at the Top Secret/Codeword level].
64. [In] a memorandum with no addressee or originator listed, noted as revised on May 9, 1996 that was found on a PCMCIA card from the Maryland residence, [Deutch discusses information at the Secret level].
65. A document with no heading or date concerning a Deutch trip was found on the hard drive of Deutch's laptop computer, which was marked for unclassified use, describes [information classified at the Secret/Codeword level].
66. A document without headings or dates, which was found on the hard drive of the unclassified computer in Deutch's 7th floor office, [discusses information classified at the Secret/Codeword level].
67. Deutch's journal, which was found on a PCMCIA card from the Maryland residence, also covered this topic but in more detail.
68. A spread sheet document [contains] financial [data] from fiscal year 1995 (FY95) through FY01 [which is classified at the Secret/compartmented program level. It was found on a PCMCIA card from the Maryland residence.

WHAT VULNERABILITIES MAY HAVE ALLOWED THE HOSTILE EXPLOITATION OF DEUTCH'S UNPROTECTED COMPUTER MEDIA?

69. The June 1994 User's Guide for PC Security, prepared by CIA's Infosec Officer Services Division, defines unclassified media as media that has never contained classified data. To maintain this status, all media and supplies related to an unclassified computer must be maintained separately from classified computer hardware, media, and supplies. Classified media is defined as media that contains or has contained classified data. It must be appropriately safeguarded from unauthorized physical (i.e., actually handling the computer) and electronic access (i.e., electronic insertion of exploitation software) that would facilitate exploitation. Computer media must be treated according to the highest classification of data ever contained on the media.

70. The Guide addresses vulnerabilities relating to computers. Word processors, other software applications, and underlying operating systems create temporary files on internal and external hard drives or their equivalents (i.e., PCMCIA cards). These temporary files are automatically created to gain additional memory for an application. When no longer needed for memory purposes, the location of the files and the data saved on the media is no longer tracked by the computer. However, the data continues to exist and is available for future recovery or unwitting transfer to other media.

71. Additionally, data contained in documents or files that are deleted by the user in a standard fashion continue to reside on magnetic media until appropriately overwritten. These deleted files and documents can be recovered with commercially available software utilities. Furthermore, computers reuse memory buffers, disk cache, and other memory and media locations (i.e., slack and free space) on storage devices without clearing all previously stored information. This results in residual data being saved in storage space allocated to new documents and files. Although this data cannot be viewed with standard software applications, it remains in memory and can be recovered.

72. As a result of these vulnerabilities, security guidelines mandate procedures to prevent unauthorized physical and electronic access to classified information. An elementary practice is to separately process classified and unclassified information. Hard drives, floppy disks, or their equivalents used in the processing of classified information must be secured in approved safes and areas approved for secure storage when not in use. Individuals having access to media that has processed classified information must possess the appropriate security clearance. Computers that process classified information and are connected to a dial-up telephone line must be protected with a cryptographic device (e.g., STU-III) approved by NSA.

What was the electronic vulnerability of Deutch's magnetic media?

73. Deutch used five government-owned Macintosh computers, configured for unclassified purposes, to process classified information. At least four of these computers were connected to modems that were lacking cryptographic devices and linked to the Internet, [an ISP], a DoD electronic mail server, and/or [bank] computers. As a result, classified information residing on Deutch's computers was vulnerable to possible electronic access and exploitation.

74. Deutch did receive e-mail on unclassified computers. One such message from France, dated July 11, 1995, was apparently from a former academic colleague who claimed to be a Russian.

75. Deutch's online identities used during his tenure as DO may have increased the risk of electronic attack. As a private subscriber [to an ISP], Deutch used a variant of his name for online identification purposes. He was also listed by true name in [the ISP's] publicly available online membership directory. This directory reflected Deutch as a user of Macintosh computers, a scientist, and as living

in Bethesda, Maryland. Similarly, Deutch's online identity associated with CIA was:

johnd@odci[Office of
DCI].gov[Government]

and with DoD, as:

deutch.johnd@odsdpo[Office of Deputy
Secretary of DefensePostOffice].secdef[Se
cretary of Defense].osd.mil[Military].

After his confirmation as DCI, Deutch's DoD user identity was unobtainable from their global address database.

76. The technical exploitation team determined that high risk Internet sites had placed "cookies"¹⁵ on the hard drives of the computers from Deutch's residences. According to DDA Calder, SIB's investigation demonstrated that the high risk material was accessed when Deutch was not present. These web sites were considered "risky" because of additional security concerns related to possible technical penetration.

What was the physical vulnerability of Deutch's magnetic media?

77. Deutch's government-issued computer at his primary residence in Maryland contained an internal hard drive and was lacking password protection. The drive was not configured for removal and secure storage when unattended even though classified information resided on the drive. Additionally, at the time of the December 17, 1996 security inspection, three of the four unsecured PCMCIA cards yielded classified information: two in PCMCIA readers and one on the desk in Deutch's study. An empty safe was also found with its drawer open.
78. Unlike his predecessors, Deutch declined a 24-hour security presence in his residence, citing concerns for personal privacy. Past practice for security staff, if present in a DCI's residence, was to assume responsibility for

securing classified information and magnetic media. To compensate for the lack of an in-house presence, CIA security personnel and local police drove by Deutch's residence on a periodic basis. The two security chiefs responsible for Deutch's protective detail stated that Deutch was responsible for securing classified information in his residence. Deutch said that he thought his residence was secure. In hindsight, he said that belief was not well founded. He said he relied, perhaps excessively, on the CIA staff and security officials to help him avoid mistakes that could result in the unauthorized disclosure of classified information.

79. On May 16, 1995, Deutch approved the installation of a residential alarm system to include an alarm on the study closet. A one-drawer safe was placed in the alarmed closet. These upgrades were completed by early June 1995.
80. According to the first Security Chief assigned to Deutch, the alarm deactivation [was provided] code to a resident alien who performed domestic work at the Maryland residence. The alien [was permitted] independent access to the residence while the Deutch's were away. CIA security database records do not reflect any security clearances being issued to the alien. The resident alien obtained U.S. citizenship during 1998.

COULD IT BE DETERMINED IF CLASSIFIED INFORMATION ON DEUTCH'S UNCLASSIFIED COMPUTER WAS COMPROMISED?

81. According to the Senior Scientist who led the technical exploitation team, there was "no clear evidence" that a compromise had occurred to information residing on storage devices used by Deutch. In a February 14, 1997 MFR, the Senior Scientist concluded:

A complete, definitive analysis, should one be warranted, would likely take many months or

longer and still not surface evidence of a data compromise.

82. On May 2, 1997, the Chief, SIB wrote in a memorandum to the Director of OPS:

In consultation with technical experts, OPS investigators determined the likelihood of compromise was actually greater via a hostile entry operation into one of Mr. Deutch's two homes (Bethesda, Maryland and Boston, Massachusetts) to "image" the contents of the affected hard drives Due to the paucity of physical security, it is stipulated that such an entry operation would not have posed a particularly difficult challenge had a sophisticated operation been launched by opposition forces The Agency computer experts advised that, given physical access to the computers, a complete "image" of the hard drives could be made in [a short amount of time].

WHAT KNOWLEDGE DID DEUTCH HAVE CONCERNING VULNERABILITIES ASSOCIATED WITH COMPUTERS?

What is Deutch's recollection?

83. During an interview with OIG, Deutch advised that, to the best of his recollection, no CIA officials had discussed with him the proper or improper use of classified and unclassified computers. Around December 1997, approximately one year after he resigned as DCI, he first became aware that computers were vulnerable to electronic attack. Not until that time, Deutch commented, had he appreciated the security risks associated with the use of a modem or the Internet in facilitating an electronic attack.¹⁶
84. Although stating that he had not received any CIA security briefings relating to the processing of information on computers, Deutch acknowledged that classified information must be properly secured when unattended. Specifically, he stated, "I am completely

conscious of the need to protect classified information."

85. In response to being advised that classified information had been recovered from government computers configured for his unclassified work, Deutch stated that he "fell into the habit of using the [CIA] unclassified system [computers] in an inappropriate fashion." He specifically indicated his regret for improperly processing classified information on the government-issued Macintosh computers that were connected to modems. Deutch acknowledged that he used these government-issued computers to access [the ISP], [his bank], the Internet, and a DoD electronic mail server.
86. Deutch indicated he had become accustomed to exclusively using an unclassified Macintosh computer while serving at DoD. He acknowledged that prior to becoming DCI, he was aware of the security principle requiring the physical separation of classified and unclassified computers and their respective information. However, he said he believed that when a file or document was deleted (i.e., dragged to the desktop trash folder), the information no longer resided on the magnetic media nor was it recoverable. Deutch maintained that it was his usual practice to create a document on his desktop computers, copy the document to an external storage device (e.g., floppy disk), and drag the initial document to the trash folder.
87. During his tenure as DCI, Deutch said that he intentionally created the most sensitive of documents on computers configured for unclassified use. Deutch stated that if these documents were created on the classified CIA computer network, CIA officials might access the system at night and inappropriately review the information. Deutch said that he had not spent a significant amount of time thinking about computer security issues.
88. Deutch advised that other individuals had

used the government computer located in the study of his Maryland residence. Deutch's wife used this computer to prepare reports relating to official travel with her husband. Additionally, [another family member] used this computer to access [a university] library. Regarding the resident alien employed at the Maryland residence, Deutch indicated that, to his knowledge, this individual never went into the study. He further believed that the resident alien normally worked while Mrs. Deutch was in the residence.

What did Deutch learn at [an] operational briefing?

89. On August 1, 1995, Deutch and several senior CIA officials receive[d] various operational briefings.
90. [During these briefings] Deutch was specifically told that data residing on a [commercial ISP network was vulnerable to a computer attack.]
91. Deutch did not have a specific recollection relating to the August 1, 1995 briefing. He could not recall making specific comments to briefers concerning his use of [his ISP] and the need to switch to another ISP.

What was Deutch's Congressional testimony?

92. On February 22, 1996, DCI Deutch testified before the Senate Select Committee on Intelligence on the subject of worldwide security threats to the United States during the post-Cold War era. During his appearance, Deutch stated:

Mr. Chairman, I conclude with the growing challenge of the security of our information systems. There are new threats that come from changing technologies. One that is of particular concern to me is the growing ease of penetration of our interlocked computer and telecommunications systems, and the

intelligence community must be in the future alert to these needs--alert to these threats.

93. On June 25, 1996, DCI Deutch testified in front of the Permanent Investigations Subcommittee of the Senate Governmental Affairs Committee. The Committee was investigating the vulnerability of government information systems to computer attacks. Deutch's testimony focused on information warfare, which he defined as unauthorized foreign penetrations and/or manipulation of telecommunications and computer network systems.

94. In his prepared statement submitted to the Committee, Deutch indicated:

like many others in this room, [I] am concerned that this connectivity and dependency [on information systems] make us vulnerable to a variety of information warfare attacks These information attacks, in whatever form, could ... seriously jeopardize our national or economic security I believe steps need to be taken to address information system vulnerabilities and efforts to exploit them. We must think carefully about the kinds of attackers that might use information warfare techniques, their targets, objectives, and methods Hacker tools are readily available on the Internet, and hackers themselves are a source of expertise for any nation or foreign terrorist organization that is interested in developing an information warfare capability We have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks.

What are the personal recollections of DCI staff members?

95. Deutch's [Executive] Assistant served in that position from February 1995 through July 1996 at DoD and CIA. [He] considered Deutch to be an "expert" computer user. [The Executive Assistant] was responsible for coordinating the preparation of computers for Deutch's use upon

his confirmation as DCI. During the transition, [the Executive Assistant] informed Deutch that the processing of classified and unclassified information required the use of separate computers to prevent the improper transfer of data. [The Executive Assistant] stated that the computer support staff at CIA went to great lengths to appropriately label Deutch's computers as either classified or unclassified in order to prevent improper use.

96. [The Executive Assistant] advised that he never informed Deutch that it was permissible to process classified information on a computer configured for unclassified use. [The Executive Assistant] stated that he was not aware that Deutch processed classified information on computers configured for unclassified use. When advised that classified material had been recovered from multiple computers used by Deutch that had been configured for unclassified purposes, [the Executive Assistant] responded that he was at a loss to explain why this had occurred.
97. [The Executive Assistant] remembered the August 1, 1995 briefing. [The Executive Assistant] said that Deutch was very concerned about information warfare and, specifically, computer systems being attacked. [The Executive Assistant] recalled that during his CIA tenure, Deutch and he became aware of efforts by [others] to attack computer systems.
98. The computer specialist who provided regular information support to Deutch while he served at DoD, was hired at Deutch's request in June 1995 to provide computer support to the DCI Area. After arriving at CIA, the computer specialist provided direct computer support to Deutch about once per week. At times, Deutch, himself, would directly contact the computer specialist for assistance.
99. The computer specialist described Deutch as a "fairly advanced" computer user who sought and used software that was considered to be above average in complexity. Deutch

was further described as having "more than a passing interest in technology" and asking complex computer-related questions. The computer specialist found that Deutch "kept you on your toes" with questions that required research [for] the answers. Deutch was also described as having a heightened interest in the subject of encryption for computers. The computer specialist recalled that all computer equipment issued to Deutch was appropriately labeled for classified or unclassified work.

100. The computer specialist remembered a conversation with Deutch on the subject of computer operating systems creating temporary documents and files. This conversation occurred while the computer specialist restored information on Deutch's computer after it had failed (i.e., crashed). Deutch watched as documents were recovered and asked how the data could be restored. Deutch was also curious about the utility software that was used to recover the documents. The computer specialist explained to Deutch that data was regularly stored in temporary files and could be recovered. Deutch appeared to be "impressed" with the recovery process.
101. During another discussion, the computer specialist recalled telling Deutch that classified information could not be moved to or processed on an unclassified computer for security reasons.
102. The computer specialist considered Deutch to be a knowledgeable Internet user who had initially utilized this medium while a member of the scientific community at the Massachusetts Institute of Technology. During September 1996 and while Deutch was still serving as DCI, the unclassified CIA Internet web page was altered by a group of Swedish hackers. During discussions with the computer specialist concerning this incident, Deutch acknowledged that the Internet afforded the opportunity for the compromise of information.
103. C/ISMS, who supervised computer support provided to Deutch from the time of his arrival

at CIA through October 1996, considered Deutch to be a computer “super user.” Deutch only sought assistance when computer equipment was in need of repair or he desired additional software. The computer support supervisor stated that all unclassified computers and PCMCIA cards that were provided for Deutch’s use had green labels indicating they were for unclassified purposes.

104. The LAN technician, who initially configured Deutch’s computers at CIA, stated that he labeled all equipment to reflect whether it was designated for classified or unclassified purposes. The technician’s stated purpose was to make it clear to Deutch what information could be processed on a particular computer given the requirement that Deutch have access to both classified and unclassified computers.

HAD DEUTCH PREVIOUSLY BEEN FOUND TO HAVE MISHANDLED CLASSIFIED INFORMATION?

105. Beginning in 1977, when he was the Director of Energy Research at the Department of Energy (DoE), Deutch had a series of positions with U.S. Government agencies that required proper handling and safeguarding of classified information to include sensitive compartmented information and DoE restricted data.
106. From 1982 to 1988, Deutch was a paid consultant to the CIA’s National Intelligence Council. In 1984, he was also under contract to the CIA’s Directorate of Intelligence, Office of Scientific Weapons and Research, serving as a member of the DCI’s Nuclear Intelligence Panel.
107. [CIA records reflect Deutch had problems before becoming Director with regard to the handling of classified information. Other specific information on security processing and practices has been deleted due to its level of classification.] Deutch served as DoD’s Undersecretary for Acquisitions and Technology and Deputy Secretary of Defense

prior to his appointment as DCI.

108. On November 21, 1995, DCI Deutch signed a CIA classified information non-disclosure agreement concerning a sensitive operation. Several provisions pertain to the proper handling of classified information and appear to be relevant to Deutch’s practices:

I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information,

I have been advised that ... negligent handling of classified information by me could cause damage or irreparable injury to the United States

I have been advised that any breach of this agreement may result in the termination of any security clearances I hold; removal from any position or special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances

I agree that I shall return all classified materials, which have, or may come into my possession or for which I am responsible because of such access ... upon the conclusion of my employment

I have read this Agreement carefully and my questions, if any, have been answered.

OIG also obtained similar, non-disclosure agreements signed by Deutch during his employment at DoD.

WHAT LAWS, REGULATIONS, AGREEMENTS, AND POLICIES HAVE POTENTIAL APPLICATION?

109. Title 18 United States Code (U.S.C.) § 793, “Gathering, transmitting or losing defense information” specifies in paragraph (f): *Whoever, being entrusted with or having lawful possession or control of any document,*

writing,...or information, relating to national defense ...through gross negligence permits the same to be removed from its proper place of custody ... shall be fined under this title or imprisoned not more than ten years, or both.

110. Title 18 U.S.C. § 798, “Disclosure of classified information” specifies in part:

Whoever, knowingly and willfully ... uses in any manner prejudicial to the safety or interest of the United States ... any classified information ...obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes ... shall be fined under this title or imprisoned not more than ten years, or both.

111. Title 18 U.S.C. § 1924, “Unauthorized removal and retention of classified documents or material” specifies:

Whoever, being an officer, employee, contractor or consultant of the United States, and, by virtue of his office, employment, position or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than \$1,000, or imprisoned for not more than one year, or both.

112. The National Security Act of 1947, CIA Act of 1949, and Executive Order (E.O.) 12333 establish the legal duty and responsibility of the DCI, as head of the United States intelligence community and primary advisor to the President and the National Security Council on national foreign intelligence, to protect intelligence sources and methods from unauthorized disclosure.

113. Director of Central Intelligence Directive (DCID) 1/ 16, effective July 19, 1988, “Security Policy for Uniform Protection of Intelligence

Processed in Automated Information Systems and Networks,” reiterates the statutory authority and responsibilities assigned to the DCI for the protection of intelligence sources and methods in Section 102 of the National Security Act of 1947, E.O.s 12333 and 12356, and National Security Decision Directive 145 and cites these authorities as the basis for the security of classified intelligence, communicated or stored in automated information systems and networks.

114. DCID 1/21, effective July 29, 1994, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs) specifies in paragraph 2:

All [Sensitive Compartmented Information] must be stored within accredited SCIFs. Accreditation is the formal affirmation that the proposed facility meets physical security standards imposed by the DCI in the physical security standards manual that supplements this directive.

115. Headquarters Regulation (HR) 10-23, Storage of Classified Information or Materials. Section C (1) specifies:

Individual employees are responsible for securing classified information or material in their possession in designated equipment and areas when not being maintained under immediate personal control in approved work areas.

116. HR 10-24, “Accountability and Handling of Collateral Classified Material,” prescribes the policies, procedures, and responsibilities associated with the accountability and handling of collateral classified material. The section concerning individual employee responsibilities states:

Agency personnel are responsible for ensuring that all classified material is handled in a secure manner and that unauthorized persons are not afforded access to such material.

-
117. HR 10-25, “Accountability and Handling of Classified Material Requiring Special Control,” sets forth policy, responsibilities, and procedures that govern the transmission, control, and storage of Restricted Data, treaty organization information, cryptographic materials, and Sensitive Compartmented Information. The section states:

Individuals authorized access to special control materials are responsible for observing the security requirements that govern the transmission, control, and storage of said materials. Further, they are responsible for ensuring that only persons having appropriate clearances or access approvals are permitted access to such materials or to the equipment and facilities in which they are stored.

HOW WAS A SIMILAR CASE HANDLED?

118. In November 1996, a senior CIA official was determined to have routinely authored CIA unique, classified documents on his personal home computer and CIA-issued laptop computer configured for unclassified use. Some of the documents were at the Secret and Top Secret/Codeword level. In addition, the senior Agency official had used both computers to visit Internet sites. In addition, the senior official’s family members had access to both computers. However, there was no way to determine if the computer hard drives had been compromised.
119. On December 12, 1996, [the] OPS Legal Advisor, referred a crimes report to the Associate General Counsel (AGC) in the CIA Office of General Counsel. On December 13, 1996, the AGC forwarded to DoJ a crimes report on this incident. In June 1997, a Personnel Evaluation Board (PEB) decided to downgrade the official from an SIS-06 to SIS-05, issue a two-year letter of reprimand including caveats against monetary and non-monetary awards and promotions, and suspend the official for 30 workdays without pay.

In addition, the PEB directed the Office of Congressional Affairs to brief the appropriate Congressional intelligence committees about this senior official’s breach of security. On September 11, 1997, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence were briefed on this incident by Executive Director David Carey.

WHAT ACTIONS DID SENIOR AGENCY OFFICIALS TAKE IN HANDLING THE DEUTCH CASE?

What actions were taken by senior Agency officials after learning of this matter?

120. After learning from O’Neil on December 17, 1996 that classified information had been discovered at Deutch’s Maryland residence, Slatkin brought the issue to the attention of Acting DCI George Tenet within one day. She asserted there were multiple discussions with Tenet over time and “everything” had his concurrence. Slatkin explained that the issue was too sensitive for her and Tenet had the responsibility for making the decisions relating to the Deutch incident. Slatkin stated she was also concerned that others may have perceived that she and O’Neil, due to their close association with Deutch, should recuse themselves from the matter. Slatkin said that Tenet gave her the responsibility for coordinating this matter. She relied on O’Neil for legal advice and Calder for a technical review.
121. Calder recalled one or possibly two “late night discussions” with Tenet concerning the Deutch incident. One meeting was to provide Tenet “the lay of the land.” At the second meeting, Tenet gave instructions for the investigation to proceed unimpeded.
122. Tenet stated he first learned of the discovery of classified information on the Maryland computer in December 1996 or January 1997 from either the Chief, DCI Security Staff

or from the C/DCI Administration. Tenet recalled that Slatkin and O'Neil got involved in deciding how to handle the issue. Tenet did not hear about any disagreements concerning the handling of this matter and believed that Slatkin and O'Neil did not want to place Tenet in the position of adjudicating a matter involving Deutch.

123. O'Neil stated that he is uncertain how he first learned of the discovery of classified information on Deutch's Maryland computer. However, according to C/DCI Administration, a meeting was held on the afternoon of December 17, 1996 with O'Neil. At that meeting, O'Neil stated Deutch was concerned about retaining his personal information before returning the four PCMCIA cards to CIA. C/DCI Administration offered a solution by offering to provide Deutch with replacement PCMCIA cards on which Deutch could transfer his personal information. O'Neil passed this suggestion to Deutch, and Deutch agreed. Afterward, the contract network engineer also talked to Deutch about copying his personal information to the new PCMCIA cards. The contract network engineer recalled Deutch wanting to review the files on the original PCMCIA cards because they contained personal information.¹⁷

124. [The] PDGC learned of the matter on the day of its discovery. Between that date, December 17, 1996, and the date SIB began its investigation, the PDGC recalled there was an ongoing dialogue involving O'Neil, Slatkin, and Calder. The PDGC stated that O'Neil kept her abreast of developments.

125. The former ADDA believes that C/DCI Administration initially apprised her of the discovery on December 26, 1996. Her first concern related to properly securing the classified information at the Deutch residence, which the C/DCI Administration said he would handle. Several days later, [she] learned that the magnetic media at the Maryland residence had been secured, although not as expeditiously as she desired. [She] stated that the PCMCIA

cards that had been in Deutch's possession were given to O'Neil.

126. The former ADDA stated that Calder, Slatkin, and O'Neil held a series of meetings to discuss how to handle the incident. She recalled other issues surfacing, such as the resident alien employed as a maid at the Deutch residence; Deutch's personal financial records being maintained on government-owned computers; "disks" Deutch carried in his shirt pocket; and other government-issued unclassified computers at Deutch's Belmont residence, the OEOB, and Headquarters that may contain classified information.

127. D/OPS was first briefed on the case by Calder, who became [his] senior focal point with the former ADDA serving as a back-up. D/OPS never discussed the case directly with either Slatkin or O'Neil. He remembered that the specific permission of Slatkin or O'Neil was needed to involve others in the case. According to D/OPS, the former ADDA believed that Slatkin and O'Neil had as their main concern the fear that sensitive and personal information contained in Deutch's journals would leak. Slatkin stated it was standard operating procedure, when dealing with sensitive investigations or operations, to review requests to involve additional individuals. She claimed it was common practice for her to review such requests with the DCI. She does not recall denying any request to involve others in this case.

128. According to C/SIB, D/OPS asked him to conduct a security investigation to determine: (1) if classified information found on Deutch's government-issued unclassified computer had been compromised, and (2) what conditions would allow a compromise to occur. C/SIB said he was to determine the "who, what, where, when, and why." C/SIB expected "noteworthy" information would be compared to the appropriate DCID security standards and adjudication would be based on SIB's findings. He recalled advising the D/OPS that classified

information on unclassified media could involve a potential violation of federal law.

129. The OPS Legal Advisor wrote in a January 7, 1997 MFR that he attended a meeting the previous day with Calder, D/OPS, C/SIB, and an SIB investigator to discuss the discovery of the classified information on the computer at Deutch's Maryland residence. Among the issues discussed were:

Acknowledgment that because this case involves former DCI Deutch, whatever actions are taken by OPS and other parties will be scrutinized very closely. Therefore, it was stressed by everyone at the meeting that the security investigation of this case must follow the same pattern established in other cases where employees have placed classified information on a computer and possibly exposed that information to access by unauthorized individuals.

130. Calder stated that the OPS Legal Advisor was strident in his concern that Deutch be treated the same as any other Agency employee and senior officials should scrupulously avoid showing special treatment to Deutch. Calder agreed that the investigation should resemble those conducted for similar violations by other Agency personnel. He stated he was concerned that he insulate the OPS/SIB personnel and the C/DCI Administration to ensure that they did not "get ground up."
131. Calder stated that he initially assumed this matter would arise again in the future, possibly with a Congressional committee. Therefore, he insisted that the case be conducted in the same manner as for any CIA employee.

How were the Maryland PCMCIA cards handled?

132. SIB sought to obtain and secure all the government-issued computer equipment and magnetic media that had been provided to Deutch, such as the computers and peripherals that were at both Deutch residences. By early January 1997, all government-issued computer

equipment and magnetic media used by Deutch had been turned over to SIB with the exception of the four PCMCIA cards that had been observed by the inspection team on December 17, 1996.

133. O'Neil recalled that a DCI Security officer brought him the four PCMCIA cards from the Maryland residence. O'Neil stated he put the PCMCIA cards in his safe and never opened the envelope that contained them. He said he gave the PCMCIA cards to Calder without argument when asked.
134. Calder recalled that O'Neil told him that Deutch wanted the PCMCIA cards destroyed. Calder advocated the position that the cards should not be tampered with and must be maintained in the event of a future leak investigation. According to Calder, O'Neil and Deutch came to realize the PCMCIA cards could not be summarily destroyed. Calder stated that he went to O'Neil on three or four occasions in an attempt to obtain the four PCMCIA cards, and it took two to three weeks to reach a satisfactory arrangement for O'Neil to surrender them.
135. The PDGC also recalled, "We had to hammer O'Neil to give the [PCMCIA] cards to Security." The PDGC believes Slatkin, whose "loyalty to Deutch was incredible," and Deutch pressured O'Neil not to allow others to have access to the personal information on the cards. The PDGC stated that she, Calder, the OPS Legal Advisor, and C/SIB "pushed the other way" and advocated that O'Neil turn the cards over to Security. C/SIB confirmed the difficulty obtaining the four PCMCIA cards in O'Neil's possession.
136. The former ADDA recalled advising Slatkin that the investigation was dragging on, and that unidentified individuals believed that this was being done purposely in order to "cover up" the event. The former ADDA told Slatkin that O'Neil's withholding of the four cards supported the "cover up" perception.

137. According to Slatkin, after the former ADDA told Slatkin about the problem with the four remaining disks, she requested a meeting with Tenet, O'Neil, and Calder. Tenet reportedly told O'Neil to surrender the PCMCIA cards to Calder. Calder stated that O'Neil claimed that, although Calder had discussed his need for the cards, Calder had never specifically asked O'Neil to turn them over. C/SIB states that Calder, in his presence, "specifically ask[ed]" O'Neil to release the PCMCIA cards. Slatkin said she would have reacted earlier if she had known of Calder's concern.

138. According to O'Neil, he, Tenet, Slatkin, and Calder had conversations over a period of several weeks on the exploitation of the PCMCIA cards and protecting Deutch's privacy. After Tenet decided on the process for handling the cards, they were delivered to Calder. O'Neil said he never refused to turn over the cards for exploitation.

139. O'Neil surrendered the four PCMCIA cards to Calder on February 3, 1997. Calder provided the cards to C/SIB on February 4, 1997.

What was the course of the Special Investigations Branch's investigation of Deutch?

140. Calder stated that, in his view, Slatkin and O'Neil did not want Deutch's name "to be besmirched" and O'Neil assumed the role of an "interlocutor." He also said that Slatkin and O'Neil were particularly sensitive that a possible vendetta would be orchestrated by security personnel as a response to interference by O'Neil and Slatkin in a previous, unrelated, joint investigation involving the DoD.¹⁸ Calder characterized his encounters with Slatkin regarding the Deutch investigation as "always difficult discussions" and that it was continually necessary to "push forward" and achieve "a negotiated peace." Slatkin, however, stated that she had no involvement in the DoD-CIA investigation except to determine why the

Acting Director and she had not been informed of the notification to DoD.

141. The OPS Legal Advisor believes Slatkin "constrained the investigative apparatus." He cited, as an example, Slatkin advocating allowing Deutch to go into the files to determine if the information was personal or belonged to the CIA. The OPS Legal Advisor stated that the policy has always been that an individual who places personal information on a government computer loses the expectation of privacy and the material reverts to the control of the government authorities. The OPS Legal Advisor stated that Calder, D/OPS, and the former ADDA tried to keep the investigation on track. Slatkin denied interfering with the investigation. She stated that she did not make any unilateral decisions about the course of the investigation. All requests made by Deutch were relayed to O'Neil, Calder, and Tenet.

142. In the early stages of SIB's investigation, Calder recalled telling Tenet there was no indication of a compromise and the investigation was proceeding. Calder said that the investigators showed him some of the classified material. It included Top Secret/[Codeword] information; collection methods and imagery; and possibly information identifying CIA operations officers.

143. Calder stated that after a complete package of Deutch's material was recovered from the magnetic media, the question arose as to the proper person to review the material. Because the material contained personal information, Calder recalled that Deutch wanted to review the material himself or have O'Neil do the review. Ultimately, Slatkin selected D/OPS for the task.

144. As part of the SIB investigation, C/SIB interviewed staff from DCI Security and the DCI Information Services Management Staff; he also planned to interview [Deutch's Executive Assistant] and Deutch.¹⁹ On March 24, 1997, Calder informed C/SIB that C/SIB

would not be the one to interview Deutch. (Calder later explained to OIG investigators that a concern existed to have somebody who was politically sensitive question Deutch should such an interview prove necessary.) At Calder's request, SIB composed questions to ask Deutch and, on May 15, 1997, forwarded them to D/OPS for review. However, C/SIB also informed Calder that SIB would not continue their efforts because certain interviewees (i.e., Deutch) were not accessible to SIB. Calder agreed.

145. The OPS Legal Advisor stated that, normally, a case similar to Deutch's would not only be referred to SIB for investigation, but a contemporaneous damage assessment would also be conducted. If the subject was a former employee, typically the subject would be banned from holding a security clearance and future CIA employment.

146. After D/OPS reviewed the 17,000 pages of recovered documents, he prepared a report of his findings and attached a copy of C/SIB's separate, signed report. He recalled receiving a "panicky" call from the former ADDA relaying that Slatkin wanted the report immediately.

147. Calder was familiar with D/OPS's report and stated that it was the lone document that he retained following the conclusion of the investigation. He recalled sending the report to Slatkin and receiving it back with marginal comments, possibly asking if the PCMCIA cards had been destroyed. Slatkin recalled that the draft report was hand-carried to her by Calder. After she read the report, she made written editorial comments requesting clarification and returned the draft report to either Calder or D/OPS. She received the final report, reviewed it, and personally handed it to Tenet. Tenet does not remember ever seeing D/OPS's report, nor does he recall any of the details of the report. He said it is possible that someone told him about the report or showed it to him.

148. A signed copy of the D/OPS report dated July 8, 1997, was recovered from the DDA's

Registry. It did not have any notes on the text or attached to the document. No copy was ever recovered from the DCI's Executive Registry, the Executive Director's Office, Calder's personal safe, or anywhere in OGC.

149. There was considerable discussion of what should be done with the magnetic media after its material was catalogued. O'Neil said that Tenet's decision was to retain permanently the PCMCIA cards and a copy of all the classified documents. Calder, however, said there was some disagreement among the parties and the ultimate decision was to destroy the material, including the magnetic media. At the end of the investigation, Calder remembered asking D/OPS what happened to the PCMCIA cards and being told the disks were about to be destroyed or had been destroyed. Nevertheless, Calder said he was not certain the cards were destroyed.

150. After D/OPS sent his report to Calder, the OPS Legal Advisor received an e-mail from the C/ALD stating that the PDGC had spoken to Calder about the SIB investigation of Deutch. Calder reportedly said Deutch would be given a code of conduct briefing in conjunction with Deutch's security briefing as a member of the Proliferation Commission.²⁰ On August 3, 1997, the OPS Legal Advisor sent the C/ALD an e-mail response expressing concern that no one at DoD or the White House had, so far, been notified about a possible compromise of information. He also raised the issue of Deutch retaining his security clearance. The OPS Legal Advisor wrote:

I remain unpersuaded, however, that the CIA has done everything it can in this case to protect CIA and DOD equities. The investigation has been one in name only I'm certainly not persuaded that giving this man a security clearance is in the best interest of the U.S. Government or the President I mean, jeez, when was the last time a subject of an investigation was not interviewed because he objected to talking to security officers and the EXDIR, a personal friend, used her position to

short circuit an investigation? Let's be honest with each other, this so-called investigation has been handled in a manner that was more designed not to upset friendships than to protect the interests of the U.S.G.

151. C/SIB had also relayed his concerns about the possible exposure of DoD classified material of ongoing military operations. In his chronology, C/SIB wrote that on March 14, 1997, Calder decided appropriate senior level DoD officials should be briefed on a potential compromise. Calder planned to brief Slatkin of this decision. C/SIB indicated he again reminded Calder of the need for DoD notification on March 24, 1997. The OIG investigation did not locate any information that such notification occurred until OIG notified DoD on June 17, 1998.

152. As of May 1998, when OIG began its investigation, there was no information in Deutch's official Agency security file concerning the SIB investigation or its findings nor was there any evidence of a security adjudication.

SHOULD A CRIMES REPORT INITIALLY HAVE BEEN FILED ON DEUTCH IN THIS CASE?

153. Title 28 U.S.C. § 535, "Investigation of crimes involving Government officers and employees," requires that

any information, allegation or complaint received in a department or agency of the executive branch of the government relating to violations of Title 18 [U.S. Code] involving Government officers and employees shall be expeditiously reported to the Attorney General.

154. Section 1.7(a) of E.O. 12333, United States Intelligence Activities, requires senior officials of the intelligence community to "report to the Attorney General possible violations of federal criminal laws by employees and [violations] of specified criminal laws by any other person" This responsibility is to be carried out

"as provided in procedures agreed upon by the Attorney General and the head of the department or agency concerned...."

155. Pursuant to Part 1.7(a) of E.O. 12333, the DCI and the Attorney General agreed on crimes reporting procedures for CIA on March 2, 1982. These procedures, which are included as Annex D to HR 7-1, were in effect from that time until August 2, 1995, when they were superseded by new procedures.²¹ The new procedures are contained in a document, memorandum of Understanding: Reporting of Information Concerning Federal Crimes," signed by DCI Deutch.

156. According to the Memorandum of Understanding (MOU),

[w]hen the General Counsel has received allegations, complaints, or information (hereinafter allegations) that an employee²² of the Agency may have violated, may be violating, or may violate a federal criminal statute, that General Counsel should within a reasonable period of time determine whether there is a reasonable basis²³ to believe that a federal crime has been, is being, or will be committed and that it is a crime which, under this memorandum, must be reported.²⁴

157. In [the] MFR of the OPS Legal Advisor of January 7, 1997, he wrote that another issue discussed was:

The need to determine whether a crimes report will be required after an assessment of the information stored on the drives and the PCMCIA cards. [18 U.S.C. §§ 1924 and 793(f) were briefly discussed.] The General Counsel will make any determination in that regard.

158. The OPS Legal Advisor stated that he understood that Deutch had placed classified information on unclassified CIA computers that were connected to the Internet, and the classified information only "came out of Deutch's head"

when he composed documents on the computer. The OPS Legal Advisor said he did not know or have any information that Deutch had removed documents from controlled areas containing classified information.²⁵

159. The OPS Legal Advisor remembered discussing the issue of the possible criminality of Deutch's actions with the PDGC. His position was more conservative than the PDGC's. She raised the point that, as DCI, Deutch had the legal authority to declassify material under his control. This led to her contention that Deutch could not be prosecuted for a security violation. She reportedly cited an instance when then-DCI William Casey inadvertently divulged classified information in an interview with the media.

160. The OPS Legal Advisor provided handwritten notes from January 6, 1997 about a discussion of a possible crimes report with the PDGC:

Talked to [the PDGC]. She already knew about the Deutch leak. Discussed the 793(f) issue. She concluded years ago that the DCI who has authority to declassify cannot realistically be punished under the statute. I expressed my disbelief in that analysis. Hypo - does that put the DCI beyond espionage statutes? No she says that would be a natl. security callReturned briefly to information in play. Discussed how there may have been [non-CIA controlled compartmented program material] on the computer. Doesn't this push 793(f) back into play?

161. In his OIG interview, the OPS Legal Advisor said that DoD material and Top Secret/ [the non-CIA controlled compartmented program] material would not qualify for information a DCI had the authority to declassify. He realized that a referral to the FBI would "technically not" be the same as making a crimes report to DoJ. He stated there was a tendency to discuss some cases with the FBI in order to get their procedural advice.

162. The OPS Legal Advisor had a discussion with an FBI agent then assigned to the Counterespionage Group, Counterintelligence Center (CIC), regarding the possible applicability of Title 18 U.S.C. §§ 793(f) and 1924 in the matter regarding Deutch. The OPS Legal Advisor recalled this FBI Agent believing that there had to be a physical removal of documents to constitute a violation of the statutes.

163. A two-page handwritten note of January 24, 1997, composed by the OPS Legal Advisor, reported his discussion with the FBI Agent regarding the case. The note indicated that the FBI Agent at CIC suggested that it was better to have O'Neil call the then-FBI General Counsel discuss the case.

164. The OPS Legal Advisor provided an MFR reporting a January 28, 1997 meeting with the PDGC and O'Neil to discuss the Deutch case. At that time, O'Neil indicated he anticipated calling the FBI General Counsel to tell him CIA intended to conduct an investigation of this matter unless the FBI General Counsel wanted the FBI to assert investigative authority.

165. According to O'Neil, neither he nor anyone else suggested a crimes report be filed on the Deutch matter. O'Neil said a crimes report can be made at several points during an investigation. He pointed out that, in a number of cases, CIA conducts its own investigation. Matters could also be referred to DoJ to conduct an investigation.

166. O'Neil is not certain whether he talked to the FBI agent at CIC about the Deutch matter. O'Neil has a vague recollection he called the FBI General Counsel and asked him how CIA should proceed. O'Neil described the case to the FBI General Counsel, who said that the CIA should continue its own process of looking at the matter. O'Neil believes he wrote an MFR documenting his conversation and may have given the MFR to his secretary to keep in a personal folder used for sensitive matters.²⁶

167. The FBI Agent at CIC recalled that he was told Deutch had classified information on a computer disk at his home in Maryland shortly after the matter was discovered. The FBI Agent was asked if the matter was an “811” violation.²⁷ The FBI Agent concluded there was no reason to believe that the information had been compromised to a foreign power and, therefore, the FBI did not need to get involved. The FBI Agent recalled telling someone at CIA, whose identity he does not remember, that since Deutch was involved, O’Neil may want to contact the FBI General Counsel, O’Neil’s counterpart at FBI. The FBI Agent said that he established early on in his tenure at CIA that merely telling him something did not constitute official notification of the FBI much less DoJ. He was aware that OGC had crimes reporting responsibilities, and he expected them to fulfill those responsibilities.

168. The FBI General Counsel recalled a single telephone call from O’Neil after Deutch left CIA, between February and April 1997. At that time, O’Neil told the FBI General Counsel an issue had arisen about classified information existing on some computer disks at Deutch’s home. The FBI General Counsel recalled they discussed CIA reporting requirements to the FBI under “811.” [He] believes he would have told O’Neil that not enough was known about the matter at the time. If an “811” problem surfaced after CIA had looked into the matter, CIA should refer the problem to the FBI through official CIA channels.

169. The FBI General Counsel stated that he did not consider O’Neil’s call as a submission of a crimes report because, from what he remembers being told, there was no evidence of a crime. He said that he and O’Neil spoke on the telephone several times a week, but O’Neil never made a crimes report to him. [He] said that if he thought O’Neil was giving him a crimes report, he would have told him to do it through the proper channel.

170. Calder said that if a referral should have been made to DoJ and was not, he believes the omission was not intentional. However, Calder stated the responsibility for a crimes report was O’Neil’s. Calder added that “I have never issued a crimes report and would always raise such an issue with OGC for their action.” Calder said the FBI General Counsel had informed O’Neil that DoJ would not pursue a Deutch investigation regarding misuse of the computer.

171. The PDGC had supervisory responsibility of the Litigation Division, which had the crimes reporting account in OGC at that time.²⁸ The PDGC stated she did not have a lot of hands-on experience with the mechanics of coordinating crimes reports and had never authored a crimes report. She first learned of the discovery of classified information, including Top Secret/[a non-CIA controlled compartmented program] material, on a computer in Deutch’s Maryland residence on the day of its discovery in December 1996. She remembered hearing about information regarding a covert action with [two countries] but does not recall hearing there was [codeword] or [a different codeword] information on the computer. She did not learn that the computer at his Belmont residence also contained classified information.

172. The PDGC was not aware that Deutch was deleting files from the Maryland computer in the days immediately following the discovery of the classified information. She remembered speaking with Calder about the necessity of protecting the magnetic media. Her reason for wanting to retain the magnetic media was not for evidence of a crime but to have a record should there be a need to conduct a leak investigation in the future.

173. When considering the need for a crimes report, the PDGC said she did not examine the “Memorandum of Understanding: Reporting of Information Concerning Federal Crimes.” She did not consult with any attorneys from the Internal Security Section of DoJ or with

the United States Attorneys Office. She does not remember reviewing Title 18 U.S.C. § 793(f), “Gathering, transmitting or losing defense information.” She spoke with O’Neil’s Executive Assistant²⁹ regarding the provisions of Title 18 and with the OPS Legal Advisor. She did not agree with the OPS Legal Advisor’s assertion that, because the classified information “was [only] in his [Deutch’s] head,” Deutch did not remove classified information from the Agency. The PDGC was aware that, on occasion, Deutch carried the PCMCIA cards “back and forth” with him. She did not know if the cards contained classified information. The PDGC saw no distinction between classified information on a document as opposed to being on magnetic media. She explained that she was more concerned at this time with protecting and recovering the magnetic media than considering a crimes report.

174. The PDGC reviewed the statutes she thought would be relevant and did not see all the elements present for a violation. She believed that Deutch, as DCI, was the authority for the rules concerning the handling of classified information. Because Deutch issued DCIDs on classified material, she believed he could waive the rules for himself. The PDGC recognized that the DCI cannot declassify Top Secret/ [the non-CIA controlled compartmented program] material, but said such material may be handled under the DCID rules. The PDGC stated that given the fact that this matter involved a former DCI, if she had believed a crimes report was necessary, she would have shown the draft to O’Neil and he would have had the final say as to whether a crimes report was warranted.

175. The PDGC focused on Title 18 U.S.C. §1924, “Unauthorized Removal and Retention of Classified Documents or Material.” She understood that Deutch was authorized to remove classified information and take it home since he had a safe at his residence. She stated that she did not see “intent”³⁰ by Deutch. She reasoned that “intent” was a necessary element, “otherwise everyone [inadvertently]

carrying classified information out of a CIA building would be the subject of a crimes report.” According to the PDGC, Deutch had permission to take the classified material home, and Deutch’s use of the PCMCIA cards was permissible within his residence. In the PDGC’s view, the security violation occurred when he “did not do it right” by connecting the Internet to his computer and “leaving the card in the slot.” She did not distinguish between Deutch as DCI and his actual status as an Independent Contractor when the classified information was discovered. However, she would have looked at the issue differently if she understood that the only acceptable means of safeguarding the computer would have been to remove and secure the computer’s hard drive.

176. The PDGC did not remember when she made the legal decision that a crimes report was not required. She remembered speaking with C/SIB in March 1997 about his concern that a crimes report should be filed.

177. The PDGC said that D/OPS’s report was not made available to her. Although someone in OGC would usually read OPS reports, the PDGC speculated that the D/OPS would not have shown the report to her without receiving authorization. She never thought to request a copy of the D/OPS’s report to determine if his findings were consistent with her decision not to file a crimes report. Later, after she became Acting General Counsel, the issue of her reviewing the report never arose, and she would have expected OPS to raise the report with her only if the facts had changed significantly from what she learned initially.

178. In comparing the Deutch case to a similar case involving a senior Agency official, the PDGC asserted that the other official did not have a safe in his residence and was not authorized to take home classified information. She viewed this dissimilarity as a major distinction. Nor did he have the authority to waive the rules on the handling of classified information. The PDGC did not remember

if OGC made a crimes report on that case of mishandling classified information.³¹

179. George Tenet, who was Acting DCI at the time of the OPS/SIB investigation, said no one ever raised the issue of reporting this incident to DoJ, and it did not occur to him to do so. Tenet said no one ever came forward with a legal judgment that what had occurred was a crime. In Tenet's opinion, based upon what he knew at that time, there was no intent on Deutch's part to compromise classified information. Therefore, Tenet did not believe a crime was committed. Tenet was aware of the incident involving [another] senior Agency official but was not aware a crimes report had been filed on it.

SHOULD APPLICATION OF THE INDEPENDENT COUNSEL STATUTE HAVE BEEN CONSIDERED?

180. The fundamental purpose of the Independent Counsel statute is to ensure that serious allegations of unlawful conduct by certain federal executive officials are subject to review by counsel independent of any incumbent administration.
181. Title 28 U.S.C. § 592, "Preliminary investigation and application for appointment of an independent counsel" cites Title 28 U.S.C. § 591, "Applicability of provisions of this chapter," as the basis for those positions who are "covered persons" under the Independent Counsel statute.
182. Title 28 U.S.C. § 591 (a), "Preliminary investigations with respect to certain covered persons," specifies:

The Attorney General shall conduct a preliminary investigation in accordance with Section 592 whenever the Attorney General receives information sufficient to constitute grounds to investigate whether any person described in subsection (b) may have violated any Federal criminal law other than a violation

*classified as a Class B or C misdemeanor or an infraction.*³²

183. Title 28 U.S.C. § 591 (b), "Persons to whom subsection (a) applies" lists:

*... the Director of Central Intelligence [and] the Deputy Director of Central Intelligence....*³³

184. Title 28 U.S.C. § 591 (d) (1), "Examination of information to determine need for preliminary investigation," "factors to be considered" specifies:

In determining ... whether grounds to investigate exist, the Attorney General shall consider only -- (A) the specificity of the information received; and (B) the credibility of the source of the information.

185. The Deputy Chief, Public Integrity Section, Criminal Division, DoJ, is responsible for the preliminary review of matters referred to DoJ under the provisions of the Independent Counsel statute. [She] explained that the provisions of the Independent Counsel statute require DoJ to review an allegation regarding a "covered person" to determine the need for preliminary investigation based only on the two factors listed above.

186. The Deputy Chief of the Public Integrity Section explained that after the CIA IG referral in March 1998, the Public Integrity Section reviewed the matter and described it in a memorandum to the Attorney General. The memorandum stated that the allegations of illegal behavior regarding former DCI Deutch were received more than one year after Deutch left office. Accordingly, under the provisions of the Independent Counsel statute, Deutch was no longer a "covered person." The Deputy Chief of the Public Integrity Section added that the allegation should have been promptly referred to DoJ by CIA personnel.

187. The OPS Legal Advisor stated that he never considered the need to refer this matter to an Independent Counsel based on Deutch's status as a "covered person." Nor was he aware of any other discussions on this matter.

188. The PDGC stated that the issue of Deutch being a "covered person" under the Independent Counsel legislation did not arise. She said that "she never gave a thought," to the applicability of the Independent Counsel statute, and she does not know what positions within the Agency are specified as "covered persons."

189. O'Neil stated that there was no recommendation to refer the Deutch matter to DoJ under the provisions of the Independent Counsel statute.

WERE SENIOR AGENCY OFFICIALS OBLIGATED TO NOTIFY THE CONGRESSIONAL OVERSIGHT COMMITTEES OR THE INTELLIGENCE OVERSIGHT BOARD OF THE PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD? WERE THESE ENTITIES NOTIFIED?

190. Pursuant to the National Security Act of 1947, as amended, the President and the DCI bear statutory responsibility for keeping the two Congressional intelligence committees fully and currently informed of all intelligence activities.

191. Agency Regulation (AR) 7-2, "Reporting of Intelligence Activities to Congress," provides interpretation of the statutes so the Agency, with the assistance of the Office of Congressional Affairs and the Office of General Counsel, can assist the DCI in meeting the obligation to keep the intelligence committees fully and currently informed. Under the section, "Obligation to Keep Congressional Intelligence Committees Fully and Currently Informed," one of the three categories requiring reporting are:

Particular intelligence activities or categories

of activities as to which either of the Congressional intelligence committees has expressed a continuing interest (for example, potentially serious violations of U.S. criminal law by Agency employees, sources, or contacts);

192. E.O. 12863, issued September 13, 1993, President's Foreign Intelligence Advisory Board, specifies:

The heads of departments and agencies of the Intelligence Community, to the extent permitted by law, shall provide the Intelligence Oversight Board (IOB)³⁴ with all information that the IOB deems necessary to carry out its responsibilities. Inspectors General and General Counsel of the Intelligence Community, to the extent permitted by law, shall report to the IOB, at least on a quarterly basis and from time to time as necessary or appropriate, concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.

193. According to the Director of the CIA's Office of Congressional Affairs (OCA), OCA is responsible for notifications to Congress and should be informed of any formal Agency investigations. OCA receives notifications from a variety of Agency components. During Slatkin's tenure, all formal written Congressional notifications were to be routed through her office. The Director of OCA was unaware of SIB's investigation into the discovery of classified information on Deutch's government-issued unclassified computer.

194. At the January 6, 1997 meeting to discuss the planned investigation of the finding of classified information on Deutch's unclassified CIA computer, the OPS Legal Advisor stated that the Congressional oversight committees may eventually inquire about this matter. He recalled that Calder wanted the investigation performed "by the book" in case there would be a need to account for SIB actions.

195. Calder assumed this matter would again arise in the future, possibly through a leak,

with a Congressional committee. He recalled a discussion about doing briefings and was left with the impression that there was a briefing of the “Group of Four” Congressional oversight committees.³⁵

196. C/SIB maintained a chronology of the investigation consistent with Calder’s instructions. He also advised Calder, the former ADDA, the PDGC, and the D/OPS on at least two occasions that Congress, along with DoD, should be informed about the material found on Deutch’s unclassified computer. After receiving a copy of the D/OPS’s report on the investigation, C/SIB realized the report did not contain a recommendation that Congress be notified.

197. The PDGC stated she did not remember any discussion concerning notifying the Congressional oversight committees or the IOB. O’Neil said that “the question of informing the IOB or the Congressional oversight committees did not come up.”

198. Slatkin stated she could not recall any discussion or recommendation regarding the need to notify the Congressional committees about the Deutch matter. In her interview with OIG, she stated that, “surely, yes, the Committees should have been notified--but at what point?”

199. The IOB was officially notified of OIG’s investigation on May 8, 1998. After being informed of the OIG investigation, the Director of Congressional Affairs prepared talking points, which DCI Tenet presented to the SSCI and HPSC1 in early June 1998.

WHY WAS NO ADMINISTRATIVE SANCTION IMPOSED ON DEUTCH?

200. Deutch was aware that an inquiry was conducted after classified information was discovered on his government-issued computers configured for unclassified use. He said that he never tried to influence the outcome of the investigation. Nor was he told the outcome,

although he had requested that someone apprise him of the results.

201. Calder said that, despite the pressure that accompanied the investigation of a DCI, he and OPS did “the right thing.” Calder said that since Deutch was no longer a CIA employee, there was no punishment that could be administered to him. The issue was what position the Agency should take if Deutch needed access to classified information in the future. Calder was aware that Deutch’s computers had been replaced with totally unclassified magnetic media. Calder said that while Deutch was on several governmental committees, he did not believe that Deutch had a need for classified information in those positions. Calder said the remedy was to counsel Deutch in a discrete manner that would not offend his ego so he would understand the gravity of what had happened. Calder was aware that Slatkin had spoken with Deutch about the issue, and, from those conversations, Deutch would have recognized that his actions were wrong. Calder stated it was his responsibility to counsel Deutch and he planned to do so when Deutch received a briefing regarding future access. However, Calder said he never had the opportunity to meet with Deutch under the conditions he desired.

202. The former ADDA stated that she was “worn down” by Slatkin and O’Neil, and perceived that the D/OPS and Calder were similarly affected. Additionally, Calder was “frustrated” because Slatkin would not resolve issues presented to her but, instead, provided more tasking. The former ADDA said that she, the D/OPS, and Calder had reached a point where they could not go any further in that there was no additional merit in further evaluating the collected data. Slatkin had “emotional attachments” and O’Neil was not considered to be objective. According to the former ADDA, Slatkin’s and O’Neil’s oversight of the investigation was colored by a distrust of OPS and an interest to protect Deutch’s privacy. The former ADDA said that she and SIB

investigators perceived Slatkin's and O'Neil's behavior as "stonewalling." The former ADDA and SIB investigators also viewed Slatkin's requests for repeated clarifications, while typical of her management style, as a form of "pressure" to wear down the others until they were ultimately in agreement with her and O'Neil.

203. The PDGC said that there was not a "crisp end" to the case; "it ran out of steam" when many of the principals left the Agency. The PDGC thought a decision was made that the Director of the Center for CIA Security or the D/OPS would brief either Deutch or the whole Proliferation Commission regarding safeguarding classified information, but she does not know if this action was taken. O'Neil stated that after the process for producing the review was approved by the ADCI, who had been kept informed all long, he had little to do with the investigation. O'Neil also stated, he did not interfere with the OPS investigation, he left the Agency in July 1997,³⁶ and he does not know how the investigation was concluded. Slatkin said that she gave the information to Tenet and assumed that the investigation would have proceeded after she departed the Agency. The D/OPS said that, as far as he knows, no decision was ever made on what to do concerning Deutch's actions.

204. Tenet did not recall how the matter was resolved. He believes Calder, the D/OPS, Slatkin, and O'Neil had detailed discussions on the matter. Tenet was aware of concerns for Deutch's privacy. According to Tenet no one ever raised the issue of reporting the incident to the Department of Justice, or whether Deutch's clearance should be affected.

WHAT WAS OIG'S INVOLVEMENT IN THIS CASE?

When did OIG first learn of this incident?

205. The former C/DCI Administration spoke with then-IG Frederick Hitz on December 18,

1996³⁷ regarding what was found at Deutch's residence. The former C/DCI Administration described conversations he had with O'Neil and Slatkin about the matter, and O'Neil's assertion that the former C/DCI Administration was responsible for allowing Deutch to improperly process classified information. Hitz instructed the former C/DCI Administration to provide the IG with copies of any documentation,³⁸ encouraged the former C/DCI Administration to brief Tenet as soon as possible, and suggested that the former C/DCI Administration stay in contact with the IG.

206. According to the former C/DCI Administration's MFR of December 30, 1996, the IG Counsel contacted him on December 19, 1996. Reportedly, the IG Counsel urged the former C/DCI Administration to prepare an MFR and provide related documentation to the IG.

207. On December 20, 1996, Hitz called the former C/DCI Administration to inform him that he had met with Tenet, who was reportedly not aware of the Deutch matter. Hitz indicated that he and Tenet both supported the process that was being pursued on the acquisition of relevant information and the classified magnetic media. Hitz encouraged the former C/DCI Administration to ensure that his documentation was forwarded to Hitz's staff for the former C/DCI Administration's protection.

208. Hitz remembers that in mid-December 1996, the former C/DCI Administration met with him regarding classified information discovered on one or two Agency-owned computers at Deutch's residences in Maryland and Belmont. Hitz recalled the former C/DCI Administration seeking advice on what action to take. Hitz's impression was that C/DCI Administration was concerned that the former C/DCI Administration's supervisors would not act appropriately. Hitz understood that the classified information found on Deutch's computer included sensitive trip reports. The computer was connected to the Internet, and

there was [a] threat of the information being vulnerable to electronic compromise.

209. Hitz believes that he discussed the former C/DCI Administration's information with IG Counsel and the then-Deputy IG for Investigations and obtained their advice. This advice included instructing the former C/DCI Administration to secure the hard drive and other classified information that was recovered from Deutch's computers. Hitz remembered passing that instruction to the former C/DCI Administration. Hitz recalled that after meeting with IG Counsel and then-Deputy IG for Investigations, "we knew we were going to get into it and be helpful with it."

210. Hitz stated that he cannot remember what follow-up instruction he may have provided to IG Counsel and then-Deputy IG for Investigations. Hitz thinks he ultimately read the former C/DCI Administration's MFR and "did not like the smell of it" [the nature of the allegation] and "if half of what the former C/DCI Administration said was true - we would get in it." Hitz emphasized that the determination of whether to get involved would be made in concert with IG Counsel and the then-Deputy IG for Investigations. Hitz stated he never discussed the SIB investigation with Deutch, Slatkin, O'Neil, Calder, the PDGC, or D/OPS.

211. IG Counsel said that he does not remember any discussions that Hitz may have had with him and the then Deputy IG for Investigations stemming from information received from the former C/DCI Administration. The IG Counsel stated that he does not remember calling the former C/DCI Administration or having any discussion of an allegation regarding Deutch, nor does he remember seeing an MFR by the former C/DCI Administration.³⁹

212. The then-Deputy IG for Investigations said there were contacts between the former C/DCI Administration and Hitz over this issue, and Hitz would tell the then-Deputy

IG for Investigations about the conversations afterwards. The then-Deputy IG for Investigations stated he "may have detected an inference from Hitz that classified information was on the computer." However, the then-Deputy IG for Investigations did not remember any discussion with Hitz regarding the need to protect the computer's hard drive. The then-Deputy IG for Investigations was not in contact with the former C/DCI Administration.

Why did OIG wait until March 1998 to open an investigation?

213. Hitz observed that the investigation had started with the former C/DCI Administration's "security people" finding the data, and the investigation stayed in a security channel. Hitz believed that it was appropriate for that to continue as long as OPS would be allowed to do their job.

214. C/SIB's chronology noted a call from the then-Deputy IG for Investigations on January 7, 1997 asking that SIB look at a particular issue, normally the purview of the OIG (improper personal use of a government computer) to put some preliminary perspective to the issue and keep him apprised.

215. The then-Deputy IG for Investigations stated that he must have learned from Hitz that C/SIB was involved with an investigation related to Deutch and that knowledge prompted the then-Deputy IG for Investigations to call C/SIB on January 7, 1997. The then-Deputy IG for Investigations said that, if he had been informed that the matter under investigation by C/SIB was a "serious issue," he would remember it. The then-Deputy IG for Investigations categorized the issue under investigation by SIB as one of "propriety and property management." He does not recall knowing that the computers involved were intended for unclassified use.

216. The OPS Legal Advisor stated he learned

from Calder that on January 5, 1997, Hitz was briefed on the incident involving Deutch. Reportedly, Calder stated that Hitz believed that the incident was a security issue and not one for the IG. After learning of Deutch's possible appointment to the Office of Science and Technology Policy, on May 16, 1997, [the OPS Legal Advisor] wrote in an MFR that he met briefly with Hitz to discuss Deutch's possible appointment and

*Fred [Hitz] said he would speak to the DCI about this matter, and sensitize him to the problems associated with [Deutch's] needing a clearance at another U.S.G. agency. Fred asked to be kept informed.*⁴⁰

217. According to C/SIB, he contacted OIG to define OIG interests before the D/OPS began his review of the recovered documents. C/SIB met with the then-Deputy IG for Investigations, the IG Counsel, and the then-Deputy Associate IG for Investigations. C/SIB advised them that any difficulties he encountered to date were within his ability to resolve. In his chronology, C/SIB writes:

C/SIB met with [the then-Deputy IG for Investigations, the Deputy Associate IG for Investigations and the IG Counsel] re "reporting threshold" to OIG for USG Computer Misuse, both in this case in particular, and in other cases, in general. This meeting was imperative in order for C/SIB to know before the "security" review [being conducted by [the] D/OPS] what would vice would not be OIG reportable. Upon discussion, it was determined that the OIG would avail great latitude to SIB re such reporting, noting that only in instances wherein the use of the computer was obviously criminal in nature, a conflict of interests [sic] existed, an outside business was being conducted, or a private billing reimbursement for "personal entertainment" was in evidence, would the OIG require a report be submitted by SIB. (C/SIB so advised D/OPS). No particulars⁴¹ were discussed relative to SIB's ongoing

investigation, nor were any requested.

218. The then-Deputy IG for Investigations remembers the February 21, 1997 meeting with C/SIB in the presence of the Deputy Associate IG for Investigations, and possibly the IG Counsel. Up to that point, OIG had lost track of the allegation against Deutch. The then-Deputy IG for Investigations stated he told C/SIB about OIG's jurisdictional interests in terms of the computer. The then-Deputy IG for Investigations said it is possible that C/SIB made some comment about encountering some difficulty in the investigation but was working through the problem and appeared self-confident about his capability to investigate the matter. The then-Deputy IG for Investigations sensed that C/SIB was being "squeezed by unspecified OPS officials."

219. The then-Deputy IG for Investigations remembered C/SIB agreeing that he should re-contact OIG if he encountered any matter of IG interest, such as evidence of misuse of an official computer, during his investigation. According to the then-Deputy IG for Investigations, "there was no zest" on the part of OIG to take it over while OPS was working the issue. The then-Deputy IG for Investigations does not recall knowing at the time that the OPS/SIB investigation involved classified information.

220. On February 6, 1998, the Deputy Associate IG for Investigations met with C/SIB on an unrelated investigation. C/SIB incorrectly assumed the Deputy Associate IG for Investigations was investigating Deutch's mishandling of classified information on a computer at his residence. According to the Deputy Associate IG for Investigations, C/SIB disclosed that he was unable to fully pursue his investigation because of a problem with Slatkin and O'Neil. C/SIB was frustrated because there had been no interview of Deutch, a customary part of an SIB investigation.

221. During this meeting, the Deputy Associate

IG for Investigations reviewed a number of documents that included an unsigned report prepared by the D/OPS. This report detailed the D/OPS review of data discovered on the Deutch's magnetic media. The Deputy Associate IG for Investigations, subsequently met with the then-Deputy IG for Investigations, and told him what he had learned from C/SIB.

222. In his OIG interview, the then-Deputy IG for Investigations explained that OIG opened an investigation because SIB's investigation was impeded or "shutdown," and a crimes report was never sent to DoJ.

223. Hitz explained that a security violation of this nature would not normally be a matter investigated by OIG.⁴² He stated that as the IG, he would have been inclined to assert investigative authority only when he believed that the normal management response was inappropriate or not helpful. He recognized that Deutch appointees Slatkin and O'Neil were involved in the review process. Hitz stated that it was the responsibility of OIG "to support the institution."

What steps were taken by OIG after opening its investigation?

224. IG Counsel remembered advising the Deputy Associate IG for Investigations that the allegation had to be referred to DoJ as a possible crimes report. The IG Counsel also remembers a discussion about the relevance of the Independent Counsel statute since Deutch was a "covered person."

225. On March 19, 1998, OIG referred the allegations to DoJ. The crimes report letter noted that at the time of the alleged violations, Deutch was a "covered person" under the Independent Counsel statute. DoJ advised they would review the allegations for applicability to the Independent Counsel statute and further OIG investigation was not authorized until completion of DoJ's review. In May 1998, DoJ informed OIG that the Independent Counsel

statute would not apply because DoJ was not notified of the alleged violations until more than one year after Deutch left his position. As such, Deutch's status as a "covered person" had expired.

226. On May 8, 1998, OIG informed the Chairman of the Intelligence Oversight Board by letter of the criminal investigation of Deutch pursuant to E.O. 12863.

227. On June 2 and 3, 1998, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence were notified by DCI Tenet that the OIG was conducting an investigation of former DCI Deutch and the manner in which the matter was originally handled by CIA officials.

WHAT IS DEUTCH'S CURRENT STATUS WITH THE CIA?

228. Deutch's no-fee, December 1996 consulting contract was renewed in January 1998 and December 1998. The latest renewal covers the period December 16, 1998 until December 15, 1999. This contract provides Deutch with staff-like access to the Agency, its computer system, and a Top Secret clearance. Deutch's contract for the Proliferation Commission will expire when the commission finishes its work. That contract does not contain any information regarding access to classified information.

WHAT WAS THE DISPOSITION OF OIG'S CRIMES REPORT TO THE DEPARTMENT OF JUSTICE?

229. On April 14, 1999, Attorney General Janet Reno sent a letter to DCI Tenet [declining prosecution.] [The letter stated in part:]

The results of that [OIG] investigation have been reviewed for prosecutive merit and that prosecution has been declined. As I understand that Mr. Deutch currently holds a Top Secret security clearance, I suggest that the appropriate security officials at the

Central Intelligence Agency review the results of this investigation to determine Mr. Deutch's continued suitability for access to national security information.

CONCLUSIONS

- 230. Former DCI John Deutch was specifically informed that he was not authorized to process classified information on government computers configured for unclassified use.
- 231. Throughout his tenure as DCI, Deutch intentionally processed on those computers large volumes of highly classified information to include Top Secret Codeword material.
- 232. Because Deutch's computers configured for unclassified use had connections to the Internet, all classified information on those computers was at risk of compromise. Whether any of the information was stolen or compromised remains unknown.
- 233. On August 1, 1995, Deutch was made aware that computers with Internet connectivity were vulnerable to attack. Despite this knowledge, Deutch continued his practice of processing highly classified material on unclassified computers connected to the Internet.
- 234. Information developed during this investigation supports the conclusion that Deutch knew classified information remained on the hard drives of his computers even after he saved text to external storage devices and deleted the information.
- 235. Deutch misused U.S. Government computers by making extensive personal use of them. Further, he took no steps to restrict unauthorized persons from using government computers located at his residences.
- 236. The normal process for determining Deutch's continued suitability for access to classified information, to include placing the results of the SIB investigation in Deutch's security file, was not followed in this case, and no

alternative process was utilized. The standards that the Agency applies to other employees' and contractors' ability to access classified information were not applied in this case.

- 237. Because there was a reasonable basis to believe that Deutch's mishandling of classified information violated the standards prescribed by the applicable crimes reporting statute, Executive Order and Memorandum of Understanding, OGC officials Michael O'Neil and the PDGC should have submitted a crimes report to the Department of Justice.
- 238. The actions of former Executive Director Nora Slatkin and former General Counsel Michael O'Neil had the effect of delaying a prompt and thorough investigation of this matter.
- 239. DDA Richard Calder should have ensured the completion of a more thorough investigation, in particular, by arranging for an interview of Deutch and a subsequent documentation of that interview in accordance with established Agency procedures. Calder should also have ensured that the matter was brought to a conclusion rather than permitting it to languish unresolved.
- 240. Former Inspector General Frederick Hitz should have involved himself more forcefully to ascertain whether the Deutch matter raised issues for the Office of the Inspector General as well as to ensure the timely and definitive resolution of the matter.
- 241. DCI George Tenet should have involved himself more forcefully to ensure a proper resolution of this matter.
- 242. The application of the Independent Counsel statute was not adequately considered by CIA officials and, given the failure to report to DoJ on a timely basis, this in effect avoided the potential application of the statute.
- 243. The Congressional oversight committees and the Intelligence Oversight Board should have

been promptly notified of Deutch's improper handling of classified information.

Daniel S. Seikaly

RECOMMENDATIONS

1. John Deutch's continued suitability for access to classified information should be reviewed immediately.
2. The accountability of current and former Agency officials, including Deutch, for their actions and performance in connection with this matter should be determined by an appropriate panel.
3. All appropriate Agency and Intelligence Community components should be informed in writing of the sensitive information Deutch stored in his unclassified computers so that responsible authorities can take any actions that would minimize damage from possible compromise of those materials.

Aftermath of the IG Report

When the above IG report leaked to the press, it caused such consternation on Capital Hill. The SSCI initiated its own inquiry into the Deutch matter in February 2000 after becoming aware that the CIA had not actively pursued the recommendations contained in the CIA IG's report of investigation. Using the CIA IG report as foundation, the Committee sought to resolve remaining unanswered questions through more than 60 interviews with current and former Intelligence Community and law enforcement officials and a review of thousands of pages of documents. The Committee held five hearings on this topic and invited the following witnesses: CIA IG Britt Snider, Deutch, O'Neil, Slatkin, Executive Director David Carey, and DCI Tenet. O'Neil exercised his Fifth Amendment right not to testify before the Committee. In addition, former Senator Rudman, PFIAB Chairman, briefed the SSCI on the findings of the Board's report on the Deutch matter. The Committee confirmed that Deutch's unclassified computers contained summaries of

sensitive US policy discussions, references to numerous classified intelligence relationships with foreign entities, highly classified memorandums to the President, and documents imported from classified systems. As the DCI, Deutch was entrusted with protecting our nation's most sensitive secrets pursuant to the National Security Act of 1947, which charges the DCI to protect the sources and methods by which the Intelligence Community conducts its mission, the SSCI determined that he failed in this responsibility. Deutch, whose conduct should have served as the highest example, instead displayed a reckless disregard for the most basic security practices required of thousands of government employees throughout the CIA and other agencies of the Intelligence Community.

The Committee believed further that, in their response to Deutch's actions, Director Tenet, Executive Director Slatkin, General Counsel O'Neil, and other senior CIA officials failed to notify the Committee in a timely manner regarding the Deutch matter, as they are required by law. The committees were not notified of the security breach by Deutch until more than 18 months after its discovery.

The Committee determined that there were gaps in existing law that required legislative action. The law required the Inspector General to notify the Committees "immediately" if the Director or Acting Director, but not the former Director, is the subject of an Inspector General inquiry. In the Intelligence Authorization Act for Fiscal Year 2001, the Committee initiated a change in the CIA Act of 1949 to broaden the notification requirement. The new notification requirements include former DCIs, all current and former officials appointed by the President and confirmed by the Senate, the Executive Director, and the Deputy Directors for Operations, Intelligence, Administration, and Science and Technology. In addition, the Inspector General must notify the committees whenever one of the designated officials is the subject of a criminal referral to the Department of Justice. The CIA IG's July 1999 report contained three recommendations: (1) review Deutch's continued

access to classified information, (2) establish a panel to determine the accountability of current and former CIA officials with regard to the Deutch matter, (3) and advise appropriate CIA and Intelligence Community components of the sensitive information Deutch stored on his unclassified computers. DCI Tenet responded to the IG report by indefinitely suspending Deutch's security clearances and instructing Executive Director Carey to form an accountability board and to notify Intelligence Community components regarding their equities.

The Executive Director established an Agency Accountability Board in September 1999, but its first meetings were in November 1999, and subsequent sessions were not held until January 2000. Ultimately, the Deputy Director of Central Intelligence decided that the final product of the accountability board was inadequate. At his request, the PFIAB conducted an independent inquiry, and its conclusions were provided to the President and the Deputy Director.

During a Committee hearing in February 2000, DCI Tenet admitted that the CIA had not initiated a damage assessment on the possible compromise of the Deutch material. Executive Director Carey advised the Committee staff that the failure to pursue a damage assessment in August 1999 resulted from a miscommunication. This mistake was discovered in late 1999, but was not corrected until after the Committee wrote the DCI in February 2000, requesting a damage assessment be initiated.

After CIA Director Tenet revoked Deutch's intelligence clearances, the Department of Justice reconsidered its initial decision made in April 2000 not to prosecute Deutch. After another review, Justice decided to go forward with a prosecution. Before any trial began, Deutch and Justice reached a plea agreement, but it was short-circuited when President Clinton pardoned Deutch in January 2001.

Endnotes

¹ OPS was established in 1994 and was submitted as part of the new Center for CIA Security in 1998. The mission of OPS was to collect and analyze data on individuals employed by or affiliated with the Agency for the purpose of determining initial and continued reliability and suitability for access to national security information. SIB conducts investigations primarily related to suitability and internal security concerns of the Agency. SIB often works with OIG, handling initial investigations, and refers cases to the OIG and/or proper law enforcement authority once criminal conduct is detected.

² Congressional oversight is provided by the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). The two appropriations committees—the Senate Appropriations Committee, Subcommittee on Defense (SAC) and the House Appropriations Committee, National Security Subcommittee (HAC)—also bear oversight responsibilities.

³ Hereafter, the residences will be referred to as Maryland and Belmont.

⁴ This division has since been renamed the Administrative Law and Ethics Division.

⁵ According to his July 14, 1998 OIG interview, C/ALD prepared the MFR, and it was cosigned by the PDGC and (him). (He) stated that he took the only copy of it, sealed it in an envelope, and retained it. He sensed that it was likely there would eventually be an Inspector General investigation of the computer loan. (He) stated that this was the only time in his career that he has resorted to preparing such an MFR. He stated that he did not tell O'Neil about the MFR nor provide a copy to O'Neil since he judged that to be "unwise." He did not provide a copy of it to the OGC Registry. He said that he has kept it in his "hold box" since he wrote it.

⁶ The OIG investigation has not located any contract that includes a third computer.

⁷ The Infosec Officer did not copy the sixth document, a letter to DCI nominee Anthony Lake that contained Deutch's personal sentiments about senior Agency officials.

⁸ The former ADDA retired in October 1997.

⁹ Formatting prepares magnetic media for the storing and retrieval of information. Reformatting eases the tables that keep track of file locations but not the data itself, which may be recoverable.

¹⁰ OIG was unable to determine how the Belmont computer was marked because the chassis was disposed of prior to the OIG investigation.

¹¹ In response to an authorization for disclosure signed by Deutch, (the ISP) provided business records to OIG. These records reflect that Deutch, using the screen name (that was a variation of his name), maintained an account with (the ISP) since January 1, 1995.

¹² The Department of Defense recovered and produced in excess of 80 unclassified electronic message exchanges involving Deutch from May 1995 through January 1996. These messages reflect Deutch's electronic mail address as (variations of his name).

¹³ Certain material viewed by the exploitation team was described as leaving the user's computer particularly vulnerable to exploitation. The exploitation team did not recover this material and it was never viewed by OIG.

¹⁴ Journals containing classified material classified up to TS/SCI encompassing Deutch's DoD and CIA activities were recovered from multiple PCMCIA cards. Deutch stated that he believed his journals to be unclassified.

¹⁵ A "cookie" is a method by which commercial Web sites develop a profile of potential consumers by inserting data on the user's hard drive.

¹⁶ After reading the draft ROI, Deutch's refreshed recollection is that it was in December 1996, not December 1997, that he first became aware that his computer priorities resulted in vulnerability to electronic attack.

¹⁷ In his interview with OIG, Deutch confirmed he reviewed the original PCMCIA cards to delete personal information.

¹⁸ Based on a series of intelligence leaks in the *Washington Times*, CIA's Special Investigations Branch determined that leaks were related to the distribution of intelligence reports at the Pentagon. In a routine procedure, CIA sent a letter to DoD and the Defense Intelligence Agency (DIA) to coordinate an investigation. According to Calder, the DIA nominee for Director of that organization contacted Slatkin and demanded an explanation of the CIA's actions. Subsequently, O'Neil requested that DDA Calder rescind the CIA letter. Calder states that O'Neil commented the actions of CIA security officials appeared to be "vindictive and malicious."

¹⁹ C/SIB noted that he did not review Deutch's official security file. OIG reviewed the file.

²⁰ There is no record of Deutch receiving a code of conduct briefing. The Center for CIA Security provided an SCI briefing to the Commission members on two occasions. Deutch was present for the second one-hour presentation on November 17, 1998.

²¹ Although HR 7-1 Annex D was superseded by the

MOU on August 2, 1995, the current version of HR 7-1 Annex D is dated December 23, 1987 and does not reflect the changes caused by the subsequent MOU.

²² According to paragraph II B.1 of the MOU, an "employee" is defined as "a staff employee, contract employee, asset, or other person or entity providing service to or acting on behalf of any agency within the Intelligence Community.

²³ According to paragraph II E. of the MOU, "'Reasonable basis' exists when there are facts and circumstances, either personally known or of which knowledge is acquired from a source believed to be reasonably trustworthy, that would cause a person of reasonable caution to believe that a crime has been, is being, or will be committed."

²⁴ Records of the Office of General Counsel indicate there were an average of 200 written crimes reports submitted to DoJ each year for the period 1995-1998.

²⁵ Title 18 U.S.C. §§793(f) and 1924 both prohibit the improper removal of "documents."

²⁶ A check of O'Neil's "sensitive personal file" was conducted by his secretary's successor in OGC. There was no evidence of any document regarding contact between O'Neil and the FBI General Counsel concerning a possible crimes report on Deutch.

²⁷ "811" is Section 811 of the Counterintelligence and Security Enhancement Act of 1994.

²⁸ The PDGC has served in the CIA since 1982. (She) was appointed PDGC, the second highest position in the Office of General Counsel, in the summer of 1995, and serve in that capacity until March 1, 1999. While serving as PDGC, (she) also served as Acting General Counsel from August 11, 1997 until November 10, 1997.

²⁹ The then-Executive Assistant to the GC states he was aware of the inquiry regarding the classified information found on Deutch's computer and that it was being worked by others in OGC. The Executive Assistant does not remember assisting the PDGC in this matter, but concludes that, if the PDGC states that he assisted her, he has no reason to doubt her recollection.

³⁰ The statue contains the pertinent phrase "and with the intent to retain such documents or materials at an unauthorized location."

³¹ A crimes report was made by letter to DoJ on December 13, 1996. It is signed by the AGC in the Litigation Division, who was the OGC focal point for crimes reports at that time.

³² Title 18 U.S.C. §793(f) and Title 18 U.S.C. §798 are felonies; Title 18 U.S.C. §1924 is a Class A misdemeanor.

³³ Title 28 U.S.C. §591(b)(7) limits applicability of the statue to the term of office of the "covered person" and the one-year period after the individual leaves the

office or position. This means that Deutch's potential exposure to the provisions of the Independent Counsel statute expired following the one-year anniversary of his resignation, which was December 14, 1997.

³⁴ The Intelligence Oversight Board is a standing committee of the President's Foreign Intelligence Advisory Board.

³⁵ The Group of Four refers to the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, and the two appropriations committees—the Senate Appropriations Committee, the Subcommittee on Defense and the House Appropriations Committee, National Security Subcommittee.

³⁶ Although O'Neil states he left the Agency in July 1997, he was present for duty until August 11, 1997 when he was replaced by the PDGC as Acting General Counsel.

³⁷ Hitz served as CIA IG from October 12, 1990 until April 30, 1998, when he retired.

³⁸ The former C/DCI Administration provided a copy of his MFR to Hitz, Calder, and C/SIB.

³⁹ A review of Hitz's files, which he left when he retired, failed to locate (the) MFR of the former C/DCI Administration or any notes or correspondence with this investigation.

⁴⁰ Hitz corroborates the OPS Legal Advisor's account of this meeting.

⁴¹ C/SIB later explains, his use of the word "particulars" meant that he did not disclose what evidence had been discovered in his investigation. He states that it does not necessarily mean that Deutch's name and/or title was not discussed.

⁴² On February 5, 1997, Hitz sent a memorandum to the Director of Personnel Security, Subject: "Crimes Reporting and Other Referrals by Office of Personal Security to the Office of Inspector General." The memorandum eliminated the requirement for OPS to routinely notify OIG of certain specific investigative matters in which it is engaged. Included as one of the nine categories of investigative issues identified in the memorandum was the following: "Mishandling of classified information that is or could be a possible violation of 18 U.S.C. 1924, 'Unauthorized removal and retention of classified documents or material.'"

DOE Counterintelligence Failures

In the wake of the reports by the Cox Committee (see *Chapter I*) on Chinese nuclear espionage and PFIAB (see *The Rudman Report on page 343*) on security lapses at DOE's nuclear weapons laboratories, and in response to Presidential Decision Directive NSC 61,¹ a comprehensive reform of counterintelligence (CI) at DOE was undertaken. This was accelerated and significantly refined in response to legislation proposed by Congress, which, among other things, created the National Nuclear Security Agency (NNSA).

The Permanent Select Committee on Intelligence of the House of Representatives established a bipartisan investigative Panel to examine DOE's plan to improve its CI posture at its headquarters in Washington and its three key weapons laboratories. The scope of the Panel's investigation was to determine what has been done by DOE and its key constituent nuclear weapons laboratories to improve CI policy and practices in the wake of the nuclear espionage investigation at Los Alamos National Laboratory, as well as to review the status of reforms and to examine issues still unresolved or under consideration. A special staff consultant, Paul Redmond, a former chief of CI at CIA, headed the team.

Upon conclusion of its investigation into DOE security and CI issues, the Redmond Panel presented its conclusions before the Committee and provided its evaluation on the state of CI at DOE and its key weapons laboratories at Los Alamos, Sandia, and Lawrence Livermore.

In general, the review determined that DOE had made a good but inconsistent start in improving its CI capabilities. The most progress had been made in building an operational CI capability to identify and neutralize insider penetrations. The two areas of greatest shortcoming, either of which could derail the whole CI program, were in CI awareness training and in gaining employee acceptance of the polygraph program. In spite of progress in some areas, the Redmond Panel also found unsettling the statements put forth by DOE Headquarters,

claiming that counterintelligence problems had been solved. Failures and deficiencies caused by decades of misfeasance and neglect cannot be fixed overnight. The real test for assessing the CI program will be its future success in catching spies and security violators.

The Redmond Panel's report was entitled *Report of the Redmond Panel: Improving Counterintelligence Capabilities at the Department of Energy and the Los Alamos, Sandia, and Lawrence Livermore National Laboratories*, House Report No. 106-687, 21 June 2000.

R E P O R T of the REDMOND PANEL

IMPROVING COUNTERINTELLIGENCE CAPABILITIES AT THE DEPARTMENT OF ENERGY AND THE LOS ALAMOS, SANDIA, AND LAWRENCE LIVERMORE NATIONAL LABORATORIES

June 21, 2000—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
79-006 WASHINGTON: 2000

LETTER OF TRANSMITTAL

Permanent Select Committee on Intelligence,
Washington, DC, June 21, 2000.
Hon. J. Dennis Hastert,
Speaker of the House,
U.S. Capitol, Washington, DC.

Dear Mr. Speaker: Pursuant to the Rules of the House, I am pleased to transmit herewith a report submitted to the Permanent Select Committee on Intelligence of the House of Representatives by a team of investigators headed by the renowned expert in counterintelligence matters, Mr. Paul Redmond. The document is styled, "Report of the Redmond Panel: Improving Counterintelligence Capabilities at the Department of Energy and the Los Alamos, Sandia, and Lawrence Livermore National Laboratories." The Committee by majority vote earlier today authorized the filing of the report for purposes of printing.

Sincerely yours,
Porter J. Goss,
Chairman.

THE HOUSE PERMANENT SELECT
COMMITTEE ON INTELLIGENCE REPORT
OF THE REDMOND PANEL “IMPROVING
COUNTERINTELLIGENCE CAPABILITIES AT
THE DEPARTMENT OF ENERGY AND THE
LOS ALAMOS, SANDIA, AND LAWRENCE
LIVERMORE NATIONAL LABORATORIES”
FEBRUARY 2000

Executive Summary

In the wake of last year’s reports by the Cox Committee² on Chinese nuclear espionage and by the President’s Foreign Intelligence Advisory Board (PFIAB) on security lapses at the Department of Energy’s (DOE’s) nuclear weapons laboratories, and in response to Presidential Decision Directive NSC 61 (PDD-61),³ Secretary of Energy Bill Richardson embarked on a comprehensive reform of counterintelligence (CI) at DOE. This was accelerated and significantly refined in response to legislation proposed by Congress which, among other things, created the National Nuclear Security Agency (NNSA).

The House Permanent Select Committee on Intelligence established a bipartisan investigative team in the first quarter of FY 2000 to examine the Department of Energy’s plan to improve its counterintelligence posture at its headquarters in Washington and its three key weapons laboratories. The purpose of the examination was to review the status of reforms and to examine issues still unresolved or under consideration. The team was comprised of a majority staff member, a minority staff member, and a special staff consultant, Mr. Paul Redmond, one of America’s leading experts in CI and a former head of CI at the Central Intelligence Agency (CIA).

In general, the review determined that DOE has made a good but inconsistent start in improving its CI capabilities. The most progress has been made in building an operational CI capability to identify and neutralize insider penetrations. The two areas of greatest shortcoming, either of which could derail the whole CI program, are in CI awareness

training and in gaining employee acceptance of the polygraph program.

Among the specific findings and recommendations from the review are:

The current director of CI at DOE is an excellent choice for the job. Moreover, he has access to and the support of the Secretary.

DOE has failed to gain even a modicum of acceptance of the polygraph program in the laboratories. DOE must involve laboratory management in deciding who will be polygraphed.

DOE’s efforts to improve CI awareness training have failed dismally. In developing its CI awareness training program, DOE should draw on the positive experience of other U.S. government agencies, in particular the CIA and National Security Agency (NSA).

DOE also faces a considerable challenge in the area of cyber CI, that is, protecting classified and sensitive computerized media databases and communications from hostile penetration. This will require significant investment in defenses and countermeasures and require the assistance of other federal agencies.

DOE CI has established an excellent, well-staffed, and effective annual CI inspection program that will serve to ensure the maintenance of CI standards and continued improvements in the program.

The “shock therapy” of suspending the foreign visitor and assignment programs worked in making the laboratories realize the degree to which these programs, if not properly managed, can be a counterintelligence threat. The CI components at the laboratories now appear to be better involved in the process of granting approvals for visits and assignees.

Cooperation at each laboratory between CI and security personnel is largely informal and

dependent upon personal relationships. DOE and the laboratories must establish more formal mechanisms to ensure effective communication, coordination, and, most importantly, the sharing of information.

The CI offices at the laboratories are hampered by their not being cleared for access to certain Special Access Programs (SAPs). Thus, the CI components are unable to exercise CI oversight of these activities. The Director of Central Intelligence (DCI) should work with the DOE Secretary to remedy this situation.

DOE needs to establish contractual CI performance standards for the laboratories against which they can be judged and duly rewarded or penalized.

It should be noted that the Committee has not adopted the Redmond Panel's position in favor of the maintenance of the current centralization of all CI authority at DOE for a short, transitional period.

Introduction and scope of investigation

The scope of the team's investigation was to determine what has been done by the Department of Energy (DOE) and its key constituent nuclear weapons laboratories to improve counterintelligence (CI) policy and practices in the wake of the nuclear espionage investigation at Los Alamos National Laboratory. The team was limited to evaluating CI capabilities at the three principal nuclear weapons laboratories at Los Alamos, Sandia, and Lawrence Livermore, and at DOE Headquarters. The team was also to propose additional measures to improve CI at those facilities if, in the judgment of the team members, such measures were warranted.

The team interviewed DOE officials in Washington, D.C., California, and New Mexico. It also interviewed contractor employees of DOE, including employees of the University of California and Lockheed-Martin, at the three nuclear weapons laboratories. In addition, the team interviewed numerous officials of the Federal Bureau of Investigation (FBI), both at FBI Headquarters and

at FBI Field Offices in San Francisco, California and Albuquerque, New Mexico, and officials of the Central Intelligence Agency (CIA) and the National Security Agency (NSA).

This report is not linked to DOE's own progress reports, which cite percentages of CI steps that DOE considers to be "implemented" at the three weapons laboratories. The team quickly determined that DOE used imprecise terms in describing the results of its self-evaluation. For example, the word "implemented" is commonly understood to mean that something has actually been accomplished, whereas DOE considers a CI directive as implemented when it has only been promulgated. For instance, in a September 1999 progress report, DOE claimed to have implemented the recommendation that lab CI offices contact all employees and contractors who have met with foreign nationals from sensitive countries. From its on-site visits the team determined that, although the laboratory CI offices are aware of the recommendation, they have yet to carry it out. The team thus does not believe that DOE's evaluative methodology is useful in assessing the true extent to which CI measures have been "implemented."

Historical comment: In the course of interviewing numerous laboratory personnel, the team encountered a pervasive, but muted, sentiment that many of the CI and security problems at the laboratories were exacerbated, if not caused, by the policies of former Energy Secretary Hazel O'Leary. These policies included the redesign of laboratory identification badges that resulted in the intentional obscuring of distinctions between clearance levels, the collocation of Q-cleared personnel with individuals who held lesser clearances, and the widespread use of "L" clearances--which still require only the most cursory background check for approval. One senior lab official opined that the L clearance program was "the worst idea in government--cursorily clearing people who didn't need access to Q material created new vulnerabilities."

The team notes that DOE was not unique in de-emphasizing basic security procedures in the wake

of the end of the Cold War. The State Department, for example, embarked on its now infamous “no escort” policy, the Defense Intelligence Agency issued “no escort” badges to Russian military intelligence officers, and even the Central Intelligence Agency precipitously abandoned its policy of aggressively recruiting Russian intelligence officers. The present and future Administrations must ensure that such laxity will never again be encouraged or tolerated.

DOE Office of Counterintelligence (DOE CI)

Presidential Decision Directive NSC 61 (PDD 61), issued on February 11, 1998, provided for the establishment of a new DOE CI program that reports directly to the Secretary of Energy. In April 1998, DOE’s CI office became operational. Under the guidance of the director of DOE CI, Mr. Edward Curran, the Department has made considerable progress towards establishing an effective CI operational capability at DOE Headquarters to do the analytical and investigative work necessary to identify and neutralize insider penetrations. It is the team’s opinion that Mr. Curran is ideal for the CI director job because of his extensive CI experience at the FBI, his rotational assignment at the CIA, and his persistence and determination. [EDITOR’S NOTE: At the end of 2000, Ed Curran retired after rebuilding DOE’s counterintelligence program. In June 2001, Michael Waguespack was appointed to succeed Curran. Waguespack was serving as a deputy assistant director of the FBI’s National Security Division before his appointment.]

Mr. Curran appears to have access to and the support of the Secretary of Energy, which is an essential ingredient to an effective CI program. Moreover, he is vigorously attempting to exert DOE CI authority and influence over the laboratories, which, while difficult to accomplish, is critical to the success of the new CI program. In the future direct access to the Secretary and close working relations with other offices reporting directly to the Secretary, including the Offices of Security Affairs and Intelligence will be crucial. In addition, DOE CI must establish and maintain

a mutually supportive relationship with the Office of Independent Oversight and Performance Assurance, which performs inspections of DOE programs and policies. This office has an established record⁴ of detecting, documenting and reporting CI and security shortcomings at the laboratories. Regrettably, past findings of this office in the CI realm evidently were rarely acted upon. This office, which is philosophically attuned to CI and security issues, now has a good working relationship with DOE CI and has recently pointed out at least one CI cyber security⁵ vulnerability. In the future, the office will be a natural ally for DOE CI as it tries to assert authority, identify problems and implement new policies.

Mr. Curran is hiring and, where necessary, training a good cadre of CI officers to perform investigations from DOE Headquarters. The CI components at the laboratories,⁶ moreover, seem well on the way towards adequate staffing. Laboratory interaction with the FBI appears to be effective, at both the management and CI component level. That said, laboratory CI offices will need to focus for the foreseeable future on (1) gaining the confidence of their laboratory colleagues; (2) crafting CI programs that fit the unique needs of each lab; and (3) conforming to DOE’s requirements for more standardized approaches and procedures. The team appreciates that the job of reforming CI at DOE and the laboratories will require steadfast resolve on the part of Mr. Curran and his successors, continued support from the Secretary, and sustained resources from Congress.

Congressionally mandated reorganization of DOE

Mr. Curran believes that any authority he may have had in his new job as DOE’s director of CI will be greatly diluted by the new structure established in the National Defense Authorization Act for Fiscal Year 2000. While the team will not attempt to evaluate the restructuring plan, Mr. Curran’s views on the matter remain germane to the team’s evaluation of how DOE Headquarters is approaching CI reform at the laboratories.

Mr. Curran indicated to the team that his initial plan had been to place federal employees rather than contractors as the CI chief at each laboratory. This would, in his view, create a more disciplined line of authority necessary to counter the historical unresponsiveness of the laboratories to DOE Headquarters directives. Mr. Curran ultimately accepted the argument put forth by the laboratories, however, that laboratory employees, i.e., contractors, would be more acceptable locally and would thus be more effective.

Mr. Curran believes that given the semi-autonomous status of new National Nuclear Security Agency (NNSA) under the statutory restructuring, he will have only a policy role and no actual authority over these contractors. In his January 1, 2000 implementation plan, the Secretary proposed that the present director of DOE CI serve concurrently both in that capacity and as Chief of Defense Nuclear CI in the NNSA.

Separation of CI and security disciplines at the laboratory level

The deliberate separation of CI and security disciplines at the laboratories as advocated by DOE Headquarters senior management and as legislated by Congress could cause problems both at Headquarters and the laboratories. Management at each of the laboratories has sensibly placed CI and security where the expertise is. For instance, cyber security at all three laboratories resides under information management for organizational purposes. At Lawrence Livermore, the CI component resides under operations. Laboratory management and the CI chiefs appear satisfied with such arrangements. They uniformly indicated that security and CI are connected by what one Lawrence Livermore manager described as “multiple neurons” under such a rubric as an “Operational Security Group.” This group ensures that each interested or responsible component is informed and involved as issues arise.

Such claims notwithstanding, the team discovered that these “multiple-neuron-type” arrangements are not formalized in any meaningful way at

any of the three laboratories. In each case, the communications arrangements appear to depend primarily on personal and working level relationships. It has been the sad experience in many espionage cases that only after the spy is uncovered, does it become clear that a plethora of counterintelligence indicators concerning various facets of the individual’s life, performance, and behavior, had been known in different places by different individuals, but never effectively collated or holistically evaluated.

DOE must ensure that the CI officers at the laboratories are part of a formal system set up locally to ensure that all relevant CI and security data information is collected, assembled, and analyzed by means that are not solely dependent on personal relationships. Otherwise, the retirement or transfer of one individual in the process could cause the whole system to break down. Without an effective organizational structure, there is no guarantee that all relevant data will become known to the CI office.

The team is not satisfied that DOE and the laboratories have completely grasped this concept. Moreover, the DOE Operational Field offices at Albuquerque and Oakland continue to refuse to share relevant information from employee personnel files under their control with DOE CI or laboratory CI components. The team learned that DOE CI is not even informed by these three offices when an employee loses his or her security clearance. Therefore, the team recommends that DOE ensure that a formal communications process for CI information between and within the laboratories and between DOE Operational Field offices and CI personnel be established immediately.

CI inspection teams

PDD-61 requires an annual inspection of DOE’s CI program. DOE CI has hired and deployed a dozen retired FBI, CIA, and military intelligence officers to inspect the CI programs at the three weapons laboratories. This excellent initiative is already yielding promising results by identifying systemic

problems and offering solutions. The inspection team consists of highly experienced individuals, who appear to be insulated from the politicization that can yield watered down findings. The team's effectiveness, however, will be largely dependent upon the frequency of its inspections. We recommend that DOE continue annual inspections as stipulated in PDD-61 and add follow-up inspections focusing on specific problem areas. The team judges that there is no DOE CI program that is more useful or efficient than this inspection regime. We recommend, therefore, that resources adequate to expand this inspection program be provided.

The inspectors have reasonably noted that since they are just beginning their program, they should focus on establishing a baseline for assessing where the laboratory CI programs should be within a year or so. The reaction at the laboratories to these inspections has been generally favorable, with only minor complaints about repetitious questioning and an over-reliance on the format of a standard FBI internal inspection that is not entirely appropriate for this effort. Some of the CI chiefs at the laboratories believe that the inspection teams, employing a narrow FBI focus, put too much emphasis on laboratory investigative capabilities and not enough on the information gathering, non-law enforcement role of the laboratory CI units. Also, the capability of the inspection teams in the difficult, arcane cyber area needs enhancement. Overall, however, this is a fine program. With some minor adjustments, it should become an effective instrument to ensure the continued improvement of CI at the laboratories.

Polygraph testing

Polygraph testing for "covered"⁷ DOE and laboratory personnel was mandated by Congress, but DOE Headquarters reacted with poorly thought out and inconsistent directions to implement the requirement. As a result, laboratory personnel have a very negative attitude towards the polygraph. Moreover, since the polygraph is a highly visible part of the overall CI effort, the entire CI program has been negatively affected by this development. At the center of this problem is DOE's lack of

success in explaining the importance and utility of the polygraph program. Further exacerbating this problem, DOE Headquarters personnel made little effort to consider the views of senior laboratory managers and have not involved them in the planning process for determining who will be polygraphed. In addition, DOE Headquarters efforts to meet with the laboratory employees to explain the polygraph program have been ineffective, if not counterproductive. To make matters even worse, DOE Headquarters, by vacillating and changing the policy over time, appeared inconsistent and unsure where the opposite is essential to instill confidence in the program parameters and professionalism.

The attitude toward polygraphs at the laboratories runs the gamut from cautiously and rationally negative to emotionally and irrationally negative. Moreover, the attitudes of the lab directors themselves range from acknowledgement of the need (although uncertain as to how to implement it), to frank and open opposition. Scientists at Sandia prepared a scientific paper purporting to debunk the polygraph for a laboratory director's use in a Congressional hearing. Employees at Lawrence Livermore wear buttons reading "JUST SAY NO TO THE POLYGRAPH." Other laboratory employees expressed the sentiment "You trusted me to win the Cold War, now you don't?" The team heard such statements as, "The Country needs us more than we need them" and "The stock options of Silicon Valley beckon." Several expressed a belief that many scientists will quit and that DOE will not be able to maintain the stockpile stewardship program. Still more employees cited an Executive Order that exempted Presidential appointee and "Schedule C" employees from having to take the polygraph as outrageous and unfair.

In addition to the emotional reactions, there are rational questions about the polygraph, such as, "What are they going to do with the inevitable number of people who do not pass?" The team shares this concern, and expects that there will be a significant number of so-called "false-positive" polygraph results that will have to be further

examined. Another concern voiced to the team by numerous laboratory employees was that “No one has ever tried this before on this scale.” The fact is that never before have so many “cleared” employees of a government organization had to have their clearances (and, thus, their livelihoods) threatened by the institution of the polygraph.

Compounding the problem further is an attitude among many laboratory employees that they are indispensable and special, and thus, should be exempt from such demeaning and intrusive measures as the polygraph. Scientists do, in fact, represent a particular problem with regard to the administration of polygraphs. They are most comfortable when dealing with techniques that are scientifically precise and reliable. The polygraph, useful as it is as one of several tools in a CI regime, does not meet this standard. Accordingly, many scientists who have had no experience with it are skeptical of its utility.

DOE’s efforts at explaining the utility of the polygraph as part of a multi-faceted CI program have been ineffectual. Moreover, DOE Headquarters’ response to resistance at the laboratories, as unreasonable as that resistance may be, has been dictatorial and preemptory. As one senior DOE official observed, on hearing the complaint by the laboratories that the polygraph will make it difficult to recruit and retain top scientists, “It is already difficult to recruit and retain scientists in this economy, so what’s the difference?”

In December 1999, the Secretary announced that DOE intends to reduce the number of employees subject to the polygraph to about eight hundred. This change, coupled with the elimination of the exclusion for senior political appointees, indicates that DOE Headquarters is trying to rectify the original overly broad and impractical scale of the polygraph program. Nonetheless, even this well-intentioned step has elicited skepticism. As one senior manager said, “What is to prevent some new Secretary from coming along and hitting us for not polygraphing all thirteen thousand laboratory employees?”

The team judges that DOE Headquarters should do more to involve laboratory management in the process of selecting those individuals to be polygraphed. Senior laboratory managers know what secrets need protecting and, thus, could bring their knowledge to bear on this process. Including managers visibly will involve them with the program in the eyes of the workforce. This will both motivate and enable them to sell the program, and, one hopes, give the program more credibility. Their participation, moreover, would make them accountable.

To this end, DOE must reinvigorate and revamp its effort to educate the workforce on how polygraphs, while not definitive in their results, are of significant utility in a broader comprehensive CI program. The polygraph is an essential element of the CI program and it will not work until it is accepted by those who are subject to it.

Counterintelligence awareness training

There has been no discernable, effective effort from DOE Headquarters to establish and support an effective CI training and awareness program. Moreover, the team was unable to identify any real efforts on the part of DOE CI to improve upon existing DOE training and awareness practices for laboratory employees.

No organization, governmental or private, can have effective CI without active, visible, and sustained support from management and active “buy-in” by the employees. It is not possible to do CI by diktat, or from a distance. In the words of one DOE officer, the CI program cannot be a success unless each employee “knows the requirements [of the program], his or her own responsibilities, and is trained to carry them out.”

Historically, the laboratories have--on their own initiative--sponsored CI and security lectures and briefings to supplement the annual security refresher required of each employee. The CI lecture series at Lawrence Livermore is an excellent program. Unfortunately, it has not been replicated by the CI offices at Sandia or Los Alamos, which instead

sporadically arrange ad hoc presentations. Moreover, the annual security refresher, which these lectures supplement, is perfunctory and pro forma. It can consist of as little as a brief presentation on a personal computer followed by a short quiz to ensure that the employee has read the material. As a result, the refresher process is not taken seriously by the employees, especially since DOE Headquarters has dictated much of the content in the past without consulting the laboratories. The sample training materials examined by the team were bureaucratic, boring, turgid, and completely insufficient.

The poor state of the training program is also reflected in the mistaken belief by CI officials in Washington that a training facility at Kirtland Air Force Base in Albuquerque, New Mexico, is assisting in developing CI teaching materials for DOE's next annual refresher. When contacted by the team, the facility indicated that it was playing no such role. Clearly, DOE CI has yet to turn its attention to improving CI training.

In lieu of a department-wide program, the laboratories have taken some uncoordinated initiatives to meet some of their awareness training requirements, if only in response to the uproar caused by events at Los Alamos. Management at all three laboratories appears to have given some thought, at least, to what may be required. Managers have drawn an analogy between their successful occupational safety training and awareness program and how they are to make security and CI an accountable, integral part of each employee's daily work and professional mindset. At Sandia and Los Alamos, specifically, management recognizes that, as in safety management, it should give line managers specific roles and responsibilities for CI and security, and then hold them accountable. This would appear to be a constructive step.

The View from the Laboratories

Laboratory management made the following comments regarding training and awareness:

"Some of the awareness training material received from Washington is so bad it is embarrassing. Were it used, it would undermine the credibility of the whole program."

"We had to scramble to find speakers on the subject [of CI during a lab-wide CI and security stand-down]."

"One [CI] lecture given by an experienced former FBI agent, tailored to the laboratory audience, was a huge success. We need more of this sort of thing."

"There is no line budget item for training, each speaker costs about \$4,000, yet there is no Headquarters-generated program."

"DOE Headquarters' approach to training and awareness has been form over substance, represented by dictated programs and policies."

"There is an acute need for 'realistic' awareness training, so people will realize the problem did not go away with the Cold War and they are still targets."

"There are [laboratory] divisions standing in line for tailored presentations."

"Concrete examples, real [CI] incidents, and their consequences are required to get people's attention. They [the scientists] must be captured intellectually."

In the spring of 1999, the Secretary issued a series of short-notice security, CI, and cyber-related "stand-downs" at the laboratories. This was not well received by laboratory employees. Some characterized the stand-downs as a "frog marching exercise" that discredited the whole effort at improving CI by alienating significant parts of the workforce. An exception to this belief was at Los Alamos, where the stand-downs were viewed as a "unifying" experience--presumably because of the siege mentality that existed there in the wake of the nuclear espionage allegations.

The CI component at DOE Headquarters has a new training officer, and the office apparently intends to develop a program to support CI awareness and training at the laboratories. One starting point would be to follow the example of other successful CI training programs. CIA, in the aftermath of the Aldrich Ames espionage case, also instituted a very aggressive CI course and lecture program supplemented by an in-house television series. In addition, NSA has a long-standing, effective training and awareness program that the team examined at length prior to its field visits to the laboratories.

It is instructive to consider the experiences of NSA, particularly in dealing with the parts of NSA populated with an accomplished collection of world-class mathematicians and cryptologists. This highly skilled workforce is very similar to that found at the laboratories. The key factor in NSA's success in the training and awareness area appears to be that its overall integrated security and CI program has been in existence for many years, and the mathematicians enter a culture where, from the very beginning of their employment, security, CI, and the polygraph are "givens" in their daily work. DOE is now starting virtually from scratch and would do well to learn from the positive experiences of agencies such as NSA.

NSA has also had success with a program designating a security and CI referent for each significant component. This individual is not a security professional, but a regular employee of the component, one of whose additional duties involves dealing with security/CI issues. The referent, who receives some extra security and CI training, is partly rated on his performance in this role and is responsible for selling the CI program at the lowest bureaucratic level. This system, by all accounts, has been quite successful. Los Alamos has a large number of employees who are responsible for "security" in their units. Their role at Los Alamos could be expanded along the lines of the NSA model and could be adapted elsewhere. The team also notes that when it raised NSA's security/CI referent concept at each laboratory, there was widespread interest in it. Resources to enable the

laboratories to institute a referent program along the lines of the NSA model should be provided.

DOE Headquarters must do much more to support field training and awareness by establishing a comprehensive curriculum for use by the laboratories that is interesting and substantive enough to catch the attention of the difficult laboratory audience, and sufficiently flexible to allow individual CI directors to address the specific needs of each laboratory. In addition, DOE should establish a CI training course for managers. Like the successful occupational safety management training, this course should emphasize that CI is an integral part of each manager's job.

Finally, Congress should support extensive CI training and awareness programs at DOE Headquarters and the laboratories. This should include providing funds specifically for this purpose in FY 2001 to ensure that training and awareness needs are met and that money is not diverted to other programs. Congress should carefully oversee the implementation of the program it funds to ensure that training and awareness becomes, and remains, a high priority for DOE.

Cyber CI

DOE and the weapons laboratories face their biggest challenge in the area of cyber CI. The magnitude of the problem and the complexities of the issues are daunting. There are several thousand systems administrators at the laboratories who have very wide access. There are each day hundreds of thousands of internal e-mails at the laboratories and tens of thousands sent to external addresses. Additionally, there are extremely complicated issues of connectivity and systems architecture. The laboratories, wherein reside massive brainpower and experience in cyber matters, are beginning to address this challenge cooperatively and, in some cases, with the assistance of other U.S. Government agencies. Some laboratories have in place programs using "key words" to scan e-mail traffic for CI indicators, but it is too early

to formulate any substantive judgments of their effectiveness.

It is clear that DOE CI has not yet fully established its authority at DOE Headquarters and at the laboratories in the cyber area. The cyber component of DOE CI is trying to overcome legal obstacles centering largely on privacy issues related to implementation of a pilot program to determine the size and difficulty of e-mail monitoring using sophisticated “visualization” software. There is another pilot program under development to detect cyber intrusions better. DOE CI is encountering bureaucratic resistance to establishing acceptable minimum standards. For instance, the laboratories are pressing for standards that are acceptable in a more open “academic” environment. Furthermore, a comprehensive intrusion incident reporting mechanism for the computer systems controlled by DOE information management offices and the laboratories is meeting resistance from DOE and laboratory personnel, who cite excessive reporting burdens.

There has existed for years at the laboratories an entity called the Computer Incident Advisory Capability (CIAC) that was responsible for collecting and analyzing computer security incident data. The reporting to this organization has historically been voluntary, and anonymity was permitted to encourage the laboratories to be frank and forthcoming. More recently, the CIAC has begun to provide DOE Headquarters with intrusion incident summaries. The lack of specificity in these summaries, however, makes meaningful analysis impossible. DOE CI, with assistance and support from DOE management, needs to assert its authority in this matter.

It appears that DOE CI is very well served by employing detailees from the FBI and NSA. These detailees bring a high-level of expertise to the issue and some independence from DOE’s bureaucracy. The practice of assigning them to play a leading role in the cyber CI component should be continued.

The DOE CI component believes that it has an effective working relationship with DOE’s Office

of Independent Oversight and Performance Assurance. This office conducts “red team attacks” on the computer systems and has helped impose computer security standards at the laboratories. Clearly, the functions of DOE CI and this office are complementary, particularly in the cyber area. This close working relationship will be a key to improving overall cyber CI.

In sum, DOE CI, faces in the cyber area, the same very difficult, complicated issues faced everywhere in the national security community. The individuals who create and run computer systems are, by training and motivation, inclined to promote the widest, fastest, most efficient dissemination and transmission of data; hence, the basic and pervasive mutual aversion between “Chief Information Officers” and the security/CI offices. The team believes that adequate resources should be provided for cyber security and CI, and that aggressive oversight should be exercised to ensure that effective programs are developed and implemented.

Foreign visits and assignments

The team limited its examination of this issue to the role played by DOE CI and the laboratory CI offices in the visitor and assignments approval process, which would lead to the laboratory director seeking a “waiver” to the moratorium on foreign visits from sensitive countries. The team notes that Secretary Richardson announced in December 1999 that he might start seeking such waivers as permitted by the FY 2000 National Defense Authorization Act.⁸ All three laboratory CI chiefs stated that they now have an established, integrated role in the approval process leading to a laboratory director seeking a waiver to allow such a visit. For instance, the CI chief at Lawrence Livermore is one of four officers who must sign off before a request goes to the laboratory director for a decision to seek a waiver. The CI chief at Sandia is a member of the Foreign Visits and Assignments Team, which actually controls the approval process. These officials can thus bring to bear a CI perspective on any proposed visit, which the team believes to be a crucial function.

Obviously, the judgments made by the laboratory CI offices are only as good as data on which they are based. These data includes indices checks, which have often been slow in coming from other Federal agencies. The laboratory CI offices need to have access to broader-based intelligence information. This information, when integrated by the analysts in the CI offices, would give them a much improved basis on which to judge the CI threat that individual visitors and delegations might pose. Access to this information is problematic, and DOE CI needs to work with other relevant entities at DOE Headquarters—particularly the Office of Intelligence—to arrange appropriate and efficient access in the field.

In addition, there are two relevant databases. The Foreign Assignments Records Management System (FARMS) is unclassified and is maintained by DOE security. The Counterintelligence Analytical Research Data System (CARDS) is maintained by DOE CI and is an outstanding repository of classified data on prospective foreign visitors. Laboratory CI offices believe that they need a “bridge” between these databases so they can more effectively use the information they contain. In addition, it appears that the laboratories, which in some cases maintained their own databases, feel less confidence in the quality of DOE-maintained data, and their access has become more cumbersome. DOE CI needs to address these problems.

Apparently, the legislatively imposed moratorium on foreign visits and assignment has had the desired effect of making DOE and the laboratories much more conscious of the CI threat posed by visits.⁹ Making the laboratory directors accountable has also had a salutary effect. It now remains for DOE CI and the laboratory CI offices to work together to make sure the CI role in the approval process is made as effective as possible by bringing to bear the maximum amount of data as efficiently as possible. There will also need to be more awareness training to sustain and better improve the presently enhanced levels of interest and attention.

CI knowledge of special access programs (SAPs) and other sensitive projects

The laboratories do a considerable amount of work for the Intelligence Community under the auspices of the “Work-for-Others” program. This work, administered by DOE, is often highly sensitive and is administratively compartmented within SAPs, which require additional clearances. The laboratory employees who work on these SAPs or other projects technically fall under the CI jurisdiction of the laboratory CI office. The team discovered inconsistencies in this arrangement in two of the laboratories that could lead to potentially dangerous outcomes for CI if not corrected.

At Lawrence Livermore, laboratory CI officials are not permitted to become involved in the “Work-for-Others” programs involving Intelligence Community SAPs. They are not substantively or administratively informed of any aspect of the programs. Given that one of the primary functions of the laboratory CI staff is to brief employees on CI threats and to inquire about CI incidents, the CI office at Lawrence Livermore is unable to perform fully this critically important function. Lawrence Livermore’s CI chief advised that he learns of “Work for Others” activities only “by mistake” or “by accident.” In some instances when he has tried to involve himself in issues related to “Work-for-Others” activities, he has been restrained by his senior management, which presumably is seeking to enforce Intelligence Community requirements. A similar situation prevails at Sandia, where it was evident that the CI component is often unaware of “Work-for-Others” activities.¹⁰

The net result of this situation at Lawrence Livermore and Sandia is that no one appears to be examining CI issues involving personnel engaged in the most sensitive SAPs and other Intelligence Community projects without a formalized reporting mechanism, there is no guarantee that an employee will report a CI incident to the contracting intelligence agency. The contracting agency, may or may not, in turn, report the problem or issue

to the DOE Office of Intelligence, DOE CI, or to FBI Headquarters. The team judges this to be an unacceptable process for the transmission of such critical CI information. DOE Headquarters should reach a formal agreement with the Intelligence Community to ensure that the laboratory CI offices are read into the SAPs at least at an administrative level so they can fulfill their CI responsibilities. The team also encourages the Community Management Staff (CMS), which has been tasked by the Director of Central Intelligence (DCI) to examine the protection of Intelligence Community equities by DOE and the laboratories, to work closely with DOE to resolve this issue of the lack of a formalized reporting mechanism.

Sensitive unclassified technical information (SUTI)

DOE has instituted a new pseudo-classification for material that is deemed sensitive, but is technically unclassified. The team encountered significant confusion at the laboratories about what will actually be captured under the SUTI category, and laboratory managers expressed strong opposition to the whole concept. One principal argument was that scientists who work at the laboratories are already precluded from publishing much of their work because it is classified. The scientists often feel that much of what they must treat as classified is actually publicly available and being discussed by their non-U.S. Government peers around the world. Also, given that their scientific reputations are largely dependent upon what they publish and upon their interactions with their non-U.S. Government peers, they feel that the SUTI category further prejudices their ability to earn scientific recognition. Moreover, laboratory employees pointed out to the team that the SUTI category is highly subjective, cannot be standardized in any fair way, and will necessarily compel them to look for work outside of government if it is strictly imposed.

It appears that the DOE Headquarters policy on SUTI is evolving much like its policy on the polygraph, with similar misinformation, misunderstanding, and general confusion among those who will be affected by it. At Los Alamos,

senior managers advised the team that SUTI was no longer an issue because it had been replaced with a DOE list of sensitive subjects. It is interesting that Lawrence Livermore and Sandia were, at the same time, still laboring under the assumption that they would be subject to SUTI and were making decisions based upon this assumption.

In the team's judgment, DOE should proceed very cautiously and openly on SUTI imposition--if it does so at all--so as to avoid repeating the internal public relations mistakes it made with the polygraph program. Moreover, it appears DOE has yet to address the significant legal implications associated with the promulgation and implementation of SUTI. This fact was acknowledged recently by DOE's General Counsel, who issued a notice stating that since "sensitive information" is neither defined in the National Defense Authorization Act for FY 2000, nor in DOE's existing regulations, DOE will not impose new statutory penalties associated with mishandling sensitive unclassified information. Therefore, until a clear and well thought out rationale and implementation plan has been formulated by DOE for SUTI--which must include engagement with laboratory management and personnel to be effective--the team believes that steps to implement SUTI regulations should not proceed.

Enforcement

Each contract DOE has with the operators of the laboratories requires an annual appraisal of performance. In the past, these appraisals apparently included an ineffective pro forma consideration of security. It appears that neither DOE Headquarters nor DOE Field Offices, which are directly responsible for contract oversight, effectively enforced the terms of the contracts in this area. For example, the team was told that in some instances the University of California was not consciously aware of the fact that it was contractually responsible for certain security provisions, even though these were explicitly stated in the contract. The team recommends that DOE enforce existing security performance measures. Further, the team recommends that

DOE incorporate measurable CI objectives and performance standards into each of its laboratory contracts. DOE could then use the previously mentioned CI audits, possibly combined with the findings of the Office of Independent Oversight and Performance Assurance, to evaluate the performance of the laboratories and impose penalties on the contractors for unacceptable performance.

The team understands that DOE is working on language for contracts that will allow DOE to assess CI performance at the laboratories. The initiative represents an incentive for the laboratories to perform, and an opportunity to put in place measures to remedy past poor performance by the laboratories in this area. The team believes that Congress should support, encourage, and oversee the initiative, and ensure that DOE rigorously enforces the CI standards that it sets out in its contracts.

Conclusions

Hostile intelligence threats to DOE and the laboratories will most likely come from problems with trusted employees, cyber penetrations, and visitors or assignees. DOE has made good progress toward establishing effective operational mechanisms to cope with the problems of identifying possible “insider” penetrations and of laying the groundwork for the FBI to investigate. DOE has also set up an excellent inspection system to ensure the continued efficacy of these mechanisms, but it is not yet clear that this system is being evenly applied across all CI and security programs.

DOE has not effectively laid the groundwork for acceptance of the polygraph program, an obviously essential part of any CI effort to detect and deter espionage by employees. Moreover, DOE has failed to establish the absolutely key, complementary CI pillar--an effective training and awareness program.

No CI program can succeed unless both the operational and training pillars are in place and supporting each other. Further, it is clear from

decades of behavior, that the DOE and laboratory culture is profoundly antithetical toward CI and security. Unless changed, this entrenched attitude will doom any attempts at long-term improvements. Effective training and awareness programs are the only way to change this culture.

DOE is just beginning to determine the magnitude of CI issues relating to the cyber threat, which includes e-mail and intrusions. The cyber component of DOE CI needs strong support at DOE Headquarters to establish suitable, minimum CI standards in systems controlled by DOE's information management units and the laboratories.

Processes are now in place that should ensure that CI concerns will be factored into the waiver approval system for foreign visitors and assignments, questions of security in the approval process, however, were beyond the scope of this study.

In spite of progress in some areas, statements from DOE Headquarters, to the effect that all is now well in the CI area is nonsense. Problems and deficiencies caused by decades of nonfeasance and neglect cannot be fixed overnight. Such statements serve only to strengthen the position of those at the laboratories who would wait out the effort to improve CI and thus make the job all that much harder. Our yardstick for assessing the CI program will be their future success in catching spies.

Endnotes

¹ PDD-61 was issued on 11 February 1998 in response to GAO and Intelligence Community reports that found serious CI and security problems at DOE and its constituent laboratories.

² The Cox Committee's formal name was the House Select Committee on US National Security and Military/Commercial Concerns With the People's Republic of China.

³ PDD-61 was issued on 11 February 1998 in response to GAO and Intelligence Community reports that derided CI and security issues at DOE and its constituent laboratories.

⁴ In 1994, this office discovered a serious vulnerability at Los Alamos—there was no technical or policy impediment to the transfer of classified data from a classified to an unclassified computer system. This finding was apparently duly documented and reported to the requisite DOE offices and to Congress. Disturbingly, no remedial action was taken.

⁵ Cyber security is meant to encompass security for all computer systems at DOE and the laboratories.

⁶ The term “laboratories” will hereinafter include only Los Alamos, Sandia, and Lawrence Livermore National Laboratories.

⁷ Section 3154 of the FY 2000 Defense Authorization Act defines “covered” persons as those involved in Special Access Programs, Personnel Security and Assurance Programs, and Personnel Assurance Programs and those with access to Sensitive Compartmented Information.

⁸ *Washington Post*, 3 December 1999, “Energy Chief To Allow Foreign Scientist To Visit Labs.”

⁹ Evaluating the security aspects of the visits and assignments program is beyond the team's remit and is therefore not addressed herein.

¹⁰ Due to the communications arrangements between Los Alamos chiefs of intelligence, CI, and security, Los Alamos does not appear to have the same problem as Sandia and Lawrence Livermore National Laboratories.

Leaks

On 14 June 2000, the House Intelligence Committee held a hearing to review recent significant instances of the public release of classified information. The purpose of the hearing was to determine how the release of classified information has affected intelligence collection, to discuss how these cases are investigated and prosecuted, and to consider ways to halt such “leaks” of classified information. The witnesses at this hearing included Attorney General Janet Reno, DCI George Tenet, and FBI Director Louis Freeh.

Over the past five years, information regarding a number of sensitive intelligence collection programs and assets has appeared in the press. These leaks include information that endangers human intelligence sources; information about US satellite collection systems; and SIGINT information on terrorists, proliferation, and other targets.

The public release of such material usually results in the loss of access to intelligence; the enhancement of denial and deception techniques by foreign adversaries; an increased reluctance of current and potential assets to work for the United States; and the arrest, imprisonment, and execution of foreign human assets. The Bremmer Commission Report, titled “Countering the Changing Threat of International Terrorism,” stated that “[l]eaks of intelligence and law enforcement information reduce its value, endanger sources, alienate friendly nations and inhibit their cooperation, and jeopardize the US Government's ability to obtain further information.”

In most leak cases, the identity of the person who released the classified information is unknown. In many instances, the classified information was widely distributed, with literally hundreds of people having access to the intelligence report. This limits the ability of law enforcement officials to identify a possible source.

Although there are statutes prohibiting the unauthorized disclosure of certain types of information—diplomatic codes, nuclear information, communications intelligence, or “national defense” information—there is no general criminal penalty for the unauthorized disclosure of classified information. Many leaks of classified information do not easily fit within existing statutory definitions, for example, certain intelligence information from human sources and some information relating to covert action. Some legal scholars have argued that existing statutes apply to only classic espionage situations and are not meant to be applied to “leaks.”

The House Intelligence Committee sought to address this issue in the fiscal year 2001 Intelligence Authorization Bill. Section 304 of the Intelligence Authorization Act for Fiscal Year 2001 would have prohibited any current or former officer, employee, or contractor with access to “classified information” from knowingly and willfully disclosing it to unauthorized personnel. “Classified information” was defined within this section as:

. . . information or material designated and clearly marked or represented, or that the person knows or has reason to believe has been determined by appropriate authorities, pursuant to the provisions of a statute or Executive Order, as requiring protection against unauthorized disclosure for reasons of national security.

Proponents of the provision maintained that leaks of highly sensitive intelligence information had not only risk the loss of valuable collection capabilities but also jeopardized important security interests. Critics, on the other hand, argued that the provisions were overly broad and would preclude the type of leaks that in the past had ultimately benefited the American public.

After the Committee had received approval from and support for this provision from the Administration, President Clinton vetoed the Intelligence Authorization Act for Fiscal Year 2001 based upon the inclusion of this provision.

Following the veto, on 13 November 2000, the House reintroduced and passed the conference report in the House as a new bill, H.R. 5630. H.R. 5630 did not include the provision regarding “leaks” of classified information that led to the President’s veto. The Senate considered and passed H.R. 5630 on 6 December 2000, and the House passed the bill on 11 December 2000 without amendment. The President signed the bill on 27 December 2000 as P.L. 106-567.

Despite having lost on the “leak issue,” the House Intelligence Committee said it would continue its oversight of efforts to prevent and investigate unauthorized disclosures of classified information and to reintroduce legislation in the 107th Congress to address the insufficient statutory prohibitions against leaks of classified information.

Senator Richard Shelby took the lead and drafted “antileak” legislation. Senator Shelby stressed that, unlike Britain’s Official Secrets Act, his legislation targets only the “leakers.” It “criminalizes the actions of persons who are charged with protecting classified information, not those who receive or publish it.”

Opposition to Senator Shelby’s legislation pointed out that, contrary to the senator’s assurance, criminalizing disclosure of classified information has legal ramifications that went far beyond the leaker. The relevant statutes include 18 USC 2, which dictates that “Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.” This means that both the leaker and the one who elicited the leak could end up in jail.

Even the passive recipient of a leak could be in trouble if he does not immediately alert the authorities, according to 18 USC 4 (“Misprision of felony”). “Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this

title or imprisoned not more than three years, or both.”

The effort to enact a criminal statute prohibiting the unauthorized disclosure of classified information ended when a hearing on the matter was canceled and the measure was withdrawn from consideration in the FY 2002 Intelligence Authorization Act.

Senator Shelby’s office issued a terse statement:

At the request of Attorney General John Ashcroft, the Intelligence Committee has postponed Wednesday’s hearing to study the leaking of classified information. The Justice Department has requested additional time to study this issue.

Senator Shelby later commented that “This bill is going to be back in the hopper, if not by me then by others. This is not a this-year legislation, necessarily. It’s long-term legislation. This legislation is not going away, because the problem [of leaks] is going to get worse, not better.”

Timothy Steven Smith

On 8 April 2000, Federal authorities filed espionage charges against Timothy Steven Smith, a 37-year-old civilian Department of Defense employee assigned as an ordinary seaman aboard the USNS Kilauea, an ammunition ship that was moored at the time at the Puget Sound Naval Shipyard in Bremerton, Washington. Smith was accused of attempting to steal classified computer disks and documents from an officer’s cabin on the ship on 1 April, apparently in an attempt to take revenge on shipmates who had mistreated him.

One of the five classified military documents stolen by Smith detailed the transfer of ammunition and the handling of torpedoes on board US Navy ships. Smith said that he wanted to steal “valuable classified materials” and then possibly sell them over the Internet to terrorist groups.

According to the *Seattle Post Intelligencer*, Smith pleaded guilty to reduced charges. As part of his plea agreement, espionage charges initially filed against Smith were dropped, and he pleaded guilty in U.S. District Court to stealing government property and assaulting a federal officer.

The FBI said Smith admitted stealing computer disks from the first officer’s desk and fighting with crewmembers after he was caught. FBI agents found 17 computer disks in his possession, and a search of Smith’s stateroom turned up other confidential documents related to the handling of torpedoes on Navy ships. Overindulging in alcohol may have contributed to Smith’s action.

The Naval Criminal Investigative Service Field Office in Puget Sound, Washington, reported that Smith was sentenced to 260 days confinement (time served) and released on 22 December 2000.

Waguespack Leaves NACIC

Michael J. Waguespack, the National Counterintelligence Center's (NACIC) first and only Director since 1994, completed his assignment in late January 2000. During his tenure, Waguespack was the recipient of the Director of Central Intelligence's National Intelligence Medal of Achievement. On his departure, he was presented the prestigious Donovan Award by the CIA's Deputy Director of Operations, Jim Pavitt, in recognition of his contributions to the NACIC and the counterintelligence community.

He returned to FBI Headquarters where he was assigned as the Deputy Assistant Director for Counterintelligence Operations and Support, National Security Division. He remained in this position until 26 June 2001 when he was appointed Director of Counterintelligence at the Department of Energy. He replaced Ed Curran who had retired as CI Director at the end of 2000.

Jolene Hilda Neat Rector and Steven Michael Snyder

On 15 March 2001, Jolene Hilda Neat Rector and Steven Michael Snyder entered guilty pleas to a two-count indictment charging conspiracy to convey trade secrets and conveying trade secrets.

Before 20 August 1999, Rector obtained numerous pieces of proprietary information owned by R. P. Scherer, Inc. (RPS) from a friend(s) in Florida. This information included gel formulas, fill formulas, shell weights, and experimental production order data. The defendant knew that the data comprised proprietary information and trade secrets of RPS.

RPS is a leading international developer and manufacturer of drug, supplement, cosmetic, and recreational product delivery systems. RPS's proprietary advanced drug delivery systems improve the efficacy of drugs by regulating their dosage, rate of absorption, and place of release. RPS customers include global and regional manufacturers of prescription and over-the-counter pharmaceutical products, nutritional supplements, cosmetics, and recreational products such as paintballs. RPS products are produced for and placed in interstate and foreign commerce.

Sometime between 1 August and 20 August 1999, Rector requested her friend Steven Michael Snyder—then working for RPS—to send to her in Nevada the proprietary information that he had obtained from RPS. Snyder sent this information by mail, specifically including numerous experimental production orders, after Rector indicated she would use it to assist her in her current job with a competitor of RPS located in Nevada.

On 20 August 1999, Rector had a conversation with the Production Manager of Nelson Paintball, Inc. (NPB), located in Kingsford, Michigan. Rector advised him she had gelatin formulas that she wanted to sell for \$50,000. Rector stated that she had obtained the formulas while working at RPS in St. Petersburg, Florida. She also stated that she

was living in Nevada, had been working for Soft Gelcaps West (SGW), and had recently been fired. Rector said that she had worked in the paintball plant and in the nutritional plant at SGW. After the conversation, the Production Manager contacted NPB's Executive Vice President regarding Rector's phone call.

On 23 August 1999, NPB's Executive Vice President received a phone call from Rector who confirmed the previous information pertaining to the formulas and, in addition, made a number of informational statements. She told the Executive Vice President that she had 65 paintball color formulas and 108 gelatin formulas belonging to RPS that she wanted to sell them for \$50,000. The NPB Executive Vice President contacted the RPS corporate counsel office concerning Rector's information.

On 31 August 1999, the Vice President of Corporate Security for Cardinal Health (parent company of RPS) contacted the NPB Executive Vice President and asked him to contact Rector directly and have her fax a sample of the information for sale so that it could be evaluated. Following this conversation, the Executive Vice President contacted Rector and requested that she fax several of the fill and gel formulas, maintenance instructions, paintball facility layout map, and the pilot plant notebook. Approximately ten minutes later, the Executive Vice President received the requested documents.

NPB's Executive Vice President recontacted Rector to confirm receipt of the documents and then faxed what he had received to RPS. RPS then contacted the FBI, which opened an investigation on 1 September 1999. The investigation established that RPS is a Delaware corporation and a wholly owned subsidiary of Cardinal Health, Inc. Investigation further determined that Rector was employed at RPS in St. Petersburg, Florida, from April 1994 through November 1996.

On 29 September 1999, the NPB Executive Vice President initiated a consensual recorded phone call to Rector in Stagecoach, Nevada. During

this phone conversation, she advised him that she had already sold part of the documentation to an unnamed buyer; however, she was still willing to sell the remaining documentation to NPB for \$25,000.

The next day, in another consensual recorded phone call made by the Executive Vice President, Rector stated in response to his statement that she didn't sound like she wanted to come to Michigan, "Yeah, well on an illegal thing no . . . (laughing), because you know if I'm doing something that's not ill. not legally put down as like I'm doing a job . . . Yeah, then I'm setting myself up to get caught or whatever . . . you know wherever I go I'm setting myself up . . . but if there's a contract and a job, you know a job contract, then it's not a set up it, you know I'm basically doing a legal work . . . because it actually has . . . it doesn't have nobody's name on it, it is my stuff . . . "

When the Executive Vice President asked Rector what she had done with the information in the book from the pilot plant, she stated that they had rewritten it by hand and that she had destroyed the original book so that there were no names. Rector later stated that the company to whom she had sold the pharmaceutical formulas was also interested in buying the paintball formulas if she still had them.

Rector then said that she still had a maintenance manual for a Japanese Sankyo encapsulation machine, approximately 106 gel formulas, and about 60 paintball formulas to sell. Rector admitted that the examples she had faxed were from RPS.

On 14 October 1999, an undercover FBI agent met with Rector pretending to have been sent by NPB's Executive Vice President. This meeting was videotaped. Rector turned over a maroon, three-ring binder containing machine maintenance instructions, paintball and gel formulas, and list of shell weights. The undercover FBI agent then gave her a check in the amount of \$25,000.

Immediately following the exchange, the FBI agent notified Rector that the meeting had been a sting,

and she consented to be interviewed even though she had been advised that she was not under arrest and was free to go. At this time, Rector admitted that she had received an RPS notebook from a former colleague—Steven Michael Snyder—via the US mail. Furthermore, Rector advised that she had burned a lab notebook containing experimental RPS products and notes while in Kentucky.

On 26 January 2000, Rector was arrested in Nevada subsequent to a Middle District of Florida complaint and admitted having received the RPS information via the mail from a specific individual in Florida. It was this information that she had turned over to the undercover FBI agent.

Both Rector and Snyder admit that the gel formulas, fill formulas, and experimental production orders are proprietary trade secrets of RPS—developed and used by them in the production of drug, nutrient supplement and paintball delivery systems (capsules), and as the fill material inside the capsules.

Rector and Snyder's offenses constitute the first-ever prosecution under the Economic Espionage Act of 1996 in the Middle District of Florida and are part of a growing number of nationwide prosecutions under this statute since it was enacted in October 1996. This case has national significance because it reinforces the impact Congress desired to make in limiting the damage industrial espionage causes United States companies, both here and abroad.

This case also demonstrates a situation where a competitor corporation (NPB) actively cooperated with federal authorities and the victimized corporation (RPS). Without the assistance of this competitor corporation, the successful prosecution of this case would not have been possible.

The defendants face a maximum term of ten years in prison and fines up to \$250,000 for each offense.

Takashi Okamoto and Hiroaki Serizawa

On 8 May 2001, a grand jury in Cleveland, Ohio, returned a four-count indictment against Takashi Okamoto and Hiroaki Serizawa. They were charged with making false statements to the government, two counts of violating The Economic Espionage Act, and one count of Interstate Transportation of Stolen Property.

Okamoto and Serizawa met while both resided in Boston, Massachusetts, in the mid-1990s. Okamoto moved to Ohio where he gained employment with Lerner Research Institute (LRI) of the Cleveland Clinic Foundation (CCF) to conduct research into the cause and potential treatment for Alzheimer's disease in January 1997.

In January 1998, Okamoto and Serizawa, who was then employed by the Kansas University Medical Center (KUMC) in Kansas City, Kansas, began to conspire to misappropriate from the CCF certain genetic materials called Dioxyribonucleic Acid (DNA) and cell line reagents and constructs. Researchers employed by CCF, with funding provided by the CCF and the National Institutes of Health, developed these genetic materials to study the genetic cause of and possible treatment for Alzheimer's disease. Alzheimer's disease affects an estimated 4 million people in the United States alone and is the most common cause of dementia.

The indictment charges that Okamoto and Serizawa, and others known to the grand jury, provided an economic benefit and advantage to the Institute of Physical and Chemical Research (RIKEN) by giving RIKEN the DNA and cell line reagents and constructs that were misappropriated from the CCF. According to the indictment, RIKEN was a quasi-public corporation located in Saitama-Ken, Japan, which received more than 94 percent of its operational funding from the Ministry of Science and Technology of the Government of Japan. The Brain Science Institute (BSI) of RIKEN was formed in 1997 as a specific initiative of the Ministry of Science and Technology to conduct research in the area of neuroscience,

including research into the genetic cause of, and possible treatment for, Alzheimer's disease.

According to the indictment, in April 1999, RIKEN offered and Okamoto accepted a position as a neuroscience researcher to begin in the fall of 1999. The indictment charges that, on the evening of 8 July 1999 to the early morning hours of 9 July 1999, Okamoto and a third co-conspirator known as Dr. A misappropriated DNA and cell line reagents and constructs from Laboratory 164, where Okamoto conducted research at the CCF.

Also during this time, the indictment charges that Okamoto and "Dr. A" destroyed, sabotaged, and caused to be destroyed and sabotaged the DNA and cell line reagents and constructs, which they did not remove from Laboratory 164 at the CCF. The indictment further charges that, on 10 July 1999, Okamoto stored four boxes containing the stolen DNA and cell line reagents and constructs at the Cleveland, Ohio, home of "Dr. B," a colleague at the CCF with whom Okamoto was residing temporarily.

On 12 July 1999, Okamoto then retrieved the boxes of stolen DNA and cell line reagents and constructs from Dr. B's home and sent them from Cleveland, Ohio, by private interstate carrier to Serizawa at Kansas City.

On 26 July 1999, defendant Okamoto resigned from his research position at CCF and, on 3 August 1999, started his research position with RIKEN in Japan. Okamoto returned to the United States and, on 16 August 1999, retrieved the stolen DNA and cell line reagents and constructs from Serizawa's laboratory at KUMC in Kansas City.

The indictment charges that, before Okamoto left for Japan, he and Serizawa filled small laboratory vials with tap water and made meaningless markings on the labels on the vials. Okamoto instructed Serizawa to provide these worthless vials to officials at the CCF in the event they came looking for the missing DNA and cell line reagents.

On 17 August 1999, Okamoto departed the United States for Japan and carried with him the stolen DNA and cell line reagents and constructs. The last overt act charged in the conspiracy was that, in September 1999, Serizawa provided materially false, fictitious, and fraudulent statements in an interview of him by FBI special agents who were investigating the theft of the DNA and cell line reagents from the CCF.

Count two charges that the defendants committed economic espionage by stealing trade secrets that were property of the CCF, specifically, 10 DNA and cell line reagents developed through the efforts and research of researchers employed and funded by the CCF and by a grant from the National Institutes of Health.

Count three charges a violation of The Economic Espionage Act against Okamoto and Serizawa for, without authorization, altering and destroying trade secrets that were the property of CCF.

The last count of the indictment charged Okamoto and Serizawa with transporting, transmitting, and transferring DNA and cell line reagents in interstate and foreign commerce.

Ana Belen Montes

On 21 September 2001, the FBI arrested Ana Belen Montes, a US citizen born 28 February 1957, on a US military installation in Nurnberg, Germany. She was charged with spying for Cuban intelligence for the past five years.



Montes graduated with a major in Foreign Affairs from the University of Virginia in 1979 and obtained a Masters Degree from the Johns Hopkins University School of Advanced International Studies in 1988. She is single and lived alone at 3039 Macomb Street, NW, apartment 20, Washington, DC. Until her arrest, Montes was employed by the Defense Intelligence Agency (DIA) as a senior intelligence analyst. She began her employment with DIA in September 1985 and since 1992 has specialized in Cuba matters. She worked at Bolling Air Force Base in Washington, DC. Prior to joining DIA, Montes worked at the Department of Justice. In 1993, she traveled to Cuba to study the Cuban military on a CIA-paid study for the Center for the Study of Intelligence.

Communication From the Cuban Intelligence Service (CuIS) to Montes via Shortwave Radio

During a court-authorized surreptitious entry into Montes's residence, conducted by the FBI on 25 May 2001, FBI agents observed a Toshiba laptop computer.¹ During the search, the agents electronically copied the laptop's hard drive. During subsequent analysis of the copied hard

drive, the FBI recovered substantial text that had been deleted.

The recovered text from the laptop's hard drive included significant portions of a Spanish-language message, which when printed out with standard font comes to approximately 11 pages of text. The recovered portion of the message does not expressly indicate when it was composed. However, it instructs the message recipient to travel to "the Friendship Heights station" on "Saturday, November 23rd."

Although no date was on the message, November 23 fell on a Saturday in 1996. The FBI determined that this message was composed sometime before 23 November 1996 and entered onto Montes's laptop sometime after 5 October 1996, the date she purchased it. On the basis of its content, the message is from a CuIS officer to Montes.² Portions of the recovered message included the following: "You should go to the WIPE program and destroy that file according to the steps which we discussed during the contact. This is a basic step to take every time you receive a radio message or some disk."

During this same search, the agents also observed a Sony shortwave radio stored in a previously opened box on the floor of the bedroom. The agents turned on the radio to confirm that it was operable. Also found was an earpiece³ that could be utilized with this shortwave radio, allowing the radio to be listened to more privately.

The recovered portion of the message begins with the following passage:

Nevertheless, I learned that you entered the code communicating that you were having problems with radio reception. The code alone covers a lot, meaning that we do not know specifically what types of difficulty you are having. Given that it's only been a few days since we began the use of new systems, let's not rule out that the problem might be related to them. In that case, I'm going to repeat the necessary steps to take in order to retrieve a message.

The message then describes how the person reading the message should “write the information you send to us and the numbers of the radio messages which you receive.” The message later refers to going “to a new line when you get to the group 10 of the numbers that you receive via radio,” and still later gives as an “example” a series of groups of numbers: “22333 44444 77645 77647 90909 13425 76490 78399 7865498534.” After some further instruction, the message states: “Here the program deciphers the message and it retrieves the text onto the screen, asking you if the text is okay or not.” Near the conclusion of the message, there is the statement, “In this shipment you will receive the following disks: . . . 2) Disk ‘R1’ to decipher our mailings and radio.”

Further FBI analysis of Montes’s copied Toshiba hard drive identified text consisting of a series of 150 five-number groups. The text begins, “30107 24624” and continues until 150 such groups are listed. The FBI determined that the precise same numbers—in the precise same order—were broadcast on 6 February 1999 at AM frequency 7887 kHz, by a woman speaking Spanish, who introduced the broadcast with the words “Attencion! Attencion!” The frequency used in that February 1999 broadcast is within the frequency range of the shortwave radio observed in Montes’s residence on 25 May 2001.

Communication Between the CuIS and Montes via Computer Diskette⁴

Montes communicated with her CuIS handling officer by passing and receiving computer diskettes containing encrypted messages. The message described above that was contained on the hard drive of Montes’s laptop computer contained the following passage:

Continue writing along the same lines you have so far, but cipher the information every time you do, so that you do not leave prepared information that is not ciphered in the house. This is the most sensitive and compromising information that you hold. We realize that this

entails the difficulty of not being able to revise or consult what was written previously before each shipment, but we think it is worth taking this provisional measure. It is not a problem for us if some intelligence element comes repeated or with another defect which obviously cannot help, we understand this perfectly—Give “E” only the ciphered disks. Do not give, for the time being, printed or photographed material. Keep the materials which you can justify keeping until we agree that you can deliver them.—Keep up the measure of formatting the disks we send you with couriers or letters as soon as possible, leaving conventional notes as reminders only of those things to reply to or report.

The message goes on to refer to a “shipment” that contains “Disk ‘S1’—to cipher the information you send,” and, as indicated in the previous section, to “Disk ‘R1’ to decipher our mailings and radio.” Earlier in the message, there is a reference to “information you receive either via radio or disk.”

During the court-authorized search of the residence on 25 May 2001, two boxes containing a total of 16 diskettes were observed. During a subsequent search on 8 August 2001, a box containing 41 diskettes, later determined to be blank, were observed. Finally, records obtained from a Radio Shack store located near Montes’s residence indicated that Montes purchased 160 floppy diskettes during the period 1 May 1993 to 2 November 1997.

Communication From Montes to the CuIS by Pager⁵

On the basis of the evidence, Montes communicated with her handling CuIS officer using a pager. In the same message copied from Montes’s hard drive, there is a passage that states:

Beepers that you have. The only beepers in use at present are the following: 1) (917) [first seven-digit telephone number omitted from this application], use it with identification code 635. 2) (917) [second seven-digit telephone

number omitted from this application]. Use it with identification code 937. 3) (917) [third seven-digit telephone number omitted from this application] Use it only with identification code 2900 . . . because this beeper is public, in other words it is known to belong to the Cuban Mission at the UN and we assume there is some control over it. You may use this beeper only in the event you cannot communicate with those mentioned in 1) and 2), which are secure.

The reference to “control over it” in the above passage refers to the CuIS officer’s suspicion that the FBI is aware that this beeper number is associated with the Cuban Government and is monitoring it in some fashion.

In addition, the message on the laptop’s hard drive includes a portion stating that the message recipient “entered the code communicating that you were having problems with radio reception.” This portion of the message indicates that Montes at some point shortly prior to receiving the message sent a page to her CuIS officer handler consisting of a preassigned series of numbers to indicate she was having communication problems.

Montes’s Transmission of Classified Information to the CuIS

The same message described above, as well as other messages recovered from the laptop’s hard drive, contained the following information indicating that Montes had been tasked to provide and did provide classified information to the CuIS. In one portion of the message discussed above, the CuIS officer states:

*What ***⁶ said during the meeting . . . was very interesting. Surely you remember well his plans and expectations when he was coming here. If I remember right, on that occasion, we told you how tremendously useful the information you gave us from the meetings with him resulted, and how we were waiting here for him with open arms.*

The very next section in the message states:

We think the opportunity you will have to participate in the ACOM exercise in December is very good. Practically, everything that takes place there will be of intelligence value. Let’s see if it deals with contingency plans and specific targets in Cuba, which are to prioritized interests for us.

The “ACOM exercise in December” is a reference to a war games exercise in December 1996 conducted by the US Atlantic Command—a US Department of Defense unified command, in Norfolk, Virginia. Details about the exercise’s “contingency plans and specific targets” is classified Secret and relates to the national defense of the United States. DIA advised that Montes attended the above exercise in Norfolk as part of her official DIA duties.

A separate message partially recovered from the hard drive of Montes’s Toshiba laptop revealed details about a particular Special Access Program (SAP) related to the national defense of the United States:

In addition, just today the agency made me enter into a program, “special access top secret. [First name and last name omitted from this application] and I am the only ones in my office who know about the program.” [The details related about this SAP in this message are classified “Top Secret” / SCI.]

DIA has confirmed that Montes and a colleague with the same name as that related in the portion of the message described above were briefed into this SAP on 15 May 1997.

In yet another message recovered from the laptop, there is a statement revealing that “we have noticed” the location, number, and type of certain Cuban military weapons in Cuba. This information is precisely the type of information that was within Montes’s area of expertise and was,

in fact, an accurate statement of the US Intelligence Community's knowledge on this particular issue. The information is classified Secret.

FBI Physical Surveillance of Montes and Telephone Records for May to September 2001

The FBI maintained periodic physical surveillance of Montes during the period May to September 2001. On 20 May 2001, Montes left her residence and drove to the Hecht's on Wisconsin Avenue, in Chevy Chase, Maryland. She entered the store at 1:07 p.m. and exited by the rear entrance at 1:27 p.m. She then sat down on a stonewall outside the rear entrance and waited for approximately two minutes. At 1:30 p.m., the FBI observed her walk to a pay phone approximately 20 feet from where she was sitting. She placed a one-minute call to a pager number using a prepaid calling card. At 1:45 p.m., she drove out of the Hecht's lot and headed north on Wisconsin Avenue toward Bethesda, Maryland. At 1:52 p.m., she parked her car in a lot and went into Modell's Sporting Goods store. She quickly exited the store carrying a bag and crossed Wisconsin Avenue to an Exxon station.

She was observed looking over her right and left shoulders as she crossed the Exxon lot. At 2:00 p.m., she placed a one-minute call from a pay phone at the Exxon station to the same pager number using the same prepaid calling card. By 2:08 p.m., Montes had walked back to her vehicle and was driving back to her residence where she arrived at 2:30 p.m.

On 3 June 2001, Montes engaged in similar communications activity. She left her residence at approximately 2:30 p.m. and drove to a bank parking lot at the corner of Harrison Street, NW and Wisconsin Avenue, NW. She exited her car at approximately 2:37 p.m. and entered a Borders books store on Wisconsin Avenue. She left the store approximately 40 minutes later. She then crossed Wisconsin Avenue to the vicinity of three public pay phones near the southern exit of the Friendship Heights Metro Station. At 3:28 p.m., she placed a one-minute call using the same prepaid calling card

to the same pager number she had called on 20 May 2001. After a few minutes, she walked back to her car and drove to a grocery store.

Pursuant to court authorization, on 16 August 2001, the FBI searched Montes's pocketbook. In a separate compartment of Montes's wallet, the FBI found the prepaid calling card used to place the calls on 20 May 2001 and 3 June 2001. In the same small compartment, the FBI located a slip of paper on which was written the pager number she had called. Written above this pager number was a set of digits, which comprised one or more codes for Montes to use after calling the pager number; for example, after contacting the pager, she keys in a code to be sent to the pager which communicates a particular pre-established message.

On 26 August 2001, at approximately 10:00 a.m., the FBI observed Montes making a brief pay telephone call to the same pager number from a gas station/convenience store located at the intersection of Connecticut and Nebraska Avenues, NW in Washington, DC.

On September 14, 2001, Montes left work and drove directly to her residence. She then walked to Connecticut Avenue, NW, in Washington, DC., still wearing her business clothes, and made a stop at a drycleaning shop. She then entered the National Zoo through the Connecticut Avenue entrance. She proceeded to the "Prairie Land" overlook where she stayed for only 30 seconds. She then walked further into the zoo compound and basically retraced her route out of the zoo. At approximately 6:30 p.m., Montes removed a small piece of paper or card from her wallet and walked to a public phone booth located just outside the pedestrian entrance to the zoo. Montes then made what telephone records confirmed to be two calls to the same pager number she had called in May, June, and August, as described above. The records reflect that the first call was unsuccessful—the call lasted zero seconds. According to the records, she made a second call one minute later that lasted 33 seconds. Shortly after making these calls, Montes looked at her watch and then proceeded to walk back to her residence.

On 15 September 2001, telephone records pertaining to the prepaid calling card number on the card observed in her pocketbook on 16 August 2001 showed that Montes made a call to the same pager number at 11:12 a.m. that lasted one minute.

The next day—16 September—Montes left her residence in the early afternoon and took the Metro (Red Line) to the Van Ness-UDC station in Washington, DC. She made a brief telephone call from a payphone in the Metro station at approximately 1:50 p.m., again to the same pager number.

Montes owned a cell phone, which was observed during a court-authorized search of her tote bag on 16 August 2001. In addition, during surveillance on 16 September 2001, Montes was observed speaking on a cell phone. Furthermore, telephone records obtained in May 2001 confirm that she has subscribed to cell telephone service continually from 26 October 1996 to 14 May 2001. Montes's use of public pay phones notwithstanding her access to a cell phone supports the conclusion that the pay phone calls were in furtherance of Montes's espionage.

On 19 March 2002, Montes pleaded guilty to espionage in U.S. District Court in Washington, DC, and admitted that, for 16 years, she had passed top secret information to Cuban intelligence. She used shortwave radios, encrypted transmissions, and a pay telephone to contact Cuban intelligence officials and provide them the names of four US intelligence officers working in Cuba. She also informed Cuban intelligence about a US "special access program" and revealed that the US Government had uncovered the location of various Cuban military installations.

Both her defense attorney and federal prosecutors said that Montes was motivated by her moral outrage at US policy toward Cuba—an

impoverished island country—and not by money. She received only "nominal" expenses for her activities.

Although Montes could receive the death penalty for her crime, the plea agreement calls for a 25-year prison term if she cooperates with the FBI and other investigators by providing all the details she knows about Cuban intelligence activities. Judge Ricardo M. Urbina set a sentencing date of September 2002.

Endnotes

¹ A receipt obtained from a CompUSA store located in Alexandria, Virginia, indicated that, on 5 October 1996, one "Ana B. Montes" purchased a refurbished Toshiba laptop computer, model 405CS, serial number 10568512. The Toshiba laptop in her apartment had the same serial number on it as the one she purchased.

² The CuIS often communicates with clandestine CuIS agents operating outside Cuba by broadcasting encrypted messages at certain high frequencies. Under this method, the CuIS broadcasts a series of numbers on a particular frequency. The clandestine agent, monitoring the message on a shortwave radio, keys in the numbers onto a computer and then uses a diskette containing a decryption program to convert the seemingly random series of numbers into Spanish-language text. This was the methodology employed by some of the defendants convicted last June in the Southern District of Florida of espionage on behalf of Cuba and acting as unregistered agents of Cuba, in the case of *United States of America v. Gerardo Hernandez, et al.* (See *Cuban Spies in Miami*). Although it is very difficult to decrypt a message without access to the relevant decryption program, once decrypted on the agent's computer the decrypted message resides on the computer's hard drive unless the agent takes careful steps to cleanse the hard drive of the message. Simply "deleting" the file is not sufficient.

³ Similar earpieces were found in the residences of the defendants in the Hernandez case.

⁴ On the basis of knowledge of the methodology employed by the CuIS, a clandestine CuIS agent often communicates with his or her handling CuIS officer by typing a message onto a computer and then encrypting and saving it to a diskette. The agent, thereafter, physically delivers the diskette, either directly or indirectly, to the officer. In addition, as an alternative to sending an encrypted shortwave radio broadcast, a CuIS officer often will similarly place an encrypted message

onto a diskette and again simply physically deliver the diskette, clandestinely, to the agent. Upon receipt of the encrypted message, either by the CuIS officer or the agent, the recipient employs a decryption program contained on a separate diskette to decrypt the message. The exchange of diskettes containing encrypted messages, and the use of decryption programs contained on separate diskettes, was one of the clandestine communication techniques utilized by the defendants in the Hernandez case. Although it is difficult to decrypt a message without the decryption program, the very process of encrypting or decrypting a message on a computer causes a decrypted copy of the message to be placed on the computer's hard drive. Unless affirmative steps are taken to cleanse the hard drive—beyond simply “deleting” the message—the message can be retrieved from the hard drive.

⁵ On the basis of knowledge of the methodology employed by the CuIS, a clandestine CuIS agent often communicates with his or her handling CuIS officer by making calls to a pager number from a pay telephone booth and entering a preassigned code to convey a particular message. The defendants in the Hernandez case also utilized this methodology.

⁶ The FBI replaced in this application with “****” a word that begins with a capital letter, which was not translated, and is, in fact, the true last name of a US intelligence officer who was present in an undercover capacity, in Cuba, during a period that began prior to October 1996. The above quoted portion of the message indicates that Montes disclosed the US officer's intelligence agency affiliation and anticipated presence in Cuba to the CuIS, which information is classified “Secret.” As a result, the Cuban Government was able to direct its counterintelligence resources against the US officer (“we were waiting here for him with open arms”).

The Threat to Laptop Computers

The greatest threat to laptop computers comes from common thieves. A laptop is valuable, compact, very transportable, and relatively easy to steal in a public place. Police have noted that, in terms of attractiveness to criminals and their customers who purchase stolen goods, the laptop is the equivalent of the VCR and offers criminals the opportunity to exploit a whole new market—putting it at a much higher risk than the VCR that stayed at home.

A survey of 643 major corporations conducted in 2000 by the FBI and the San Francisco-based Computer Science Institute found that 60 percent of these corporations have suffered laptop thefts. Overall, nearly 320,000 laptops were stolen in the United States in 1999. According to Safeware, a computer insurance firm in Columbus, Ohio, 309,000 laptop computers were stolen in the United States during 1997—up from 208,000 in 1995—and 10 percent of all laptop thefts occurred in airports. Only virus attacks are a more prevalent security problem.

Thieves take advantage of airport hustle to steal laptops. One scam has a female accomplice tap an unsuspecting traveler on the shoulder. “You have ketchup on your shoulder,” she tells him, while handing him a tissue. The traveler puts down his laptop and dabs the messy condiment off his jacket. While he is distracted, the accomplice walks off with the laptop.

In another example, a consultant on a large project employing about a hundred other consultants traveled in and out of the same airport every weekend. Each consultant was issued the same company laptop and the same computer bag. On one occasion, the consultant believed that someone tried to switch computer bags with him but that the other individual's bag was not heavy enough to contain a computer. When the consultant yelled at the individual, he acted confused, said he was sorry, and returned the consultant's bag.

Throughout Europe, laptops are also a prime target for theft. International travelers who anticipate carrying such items should be particularly wary while transiting airports. Airports offer a particularly inviting atmosphere for laptop thieves because of large crowds, hectic schedules, and weary travelers. Laptop thefts commonly occur in places where people set them down—at security checkpoints, pay phones, lounges and restaurants, check-in lines, and restrooms.

Incidents at separate European airports demonstrate the modus operandi of thieves operating in pairs to target laptops. In the first incident, Brussels International Airport security reported that two thieves exploited a contrived delay around the security X-ray machines. The first thief preceded the traveler through the security checkpoint and then loitered around the area where security examines carry-on luggage. When the traveler placed his laptop onto the conveyer belt of the X-ray machine, the second thief stepped in front of the traveler and set off the metal detector. With the traveler now delayed, the first thief removed the traveler's laptop from the conveyer belt just after it passed through the X-ray machine and quickly disappeared.

In the second incident, a traveler walking around Frankfurt International Airport in Germany and carrying a laptop in his roll bag did not realize that a thief was walking in front of him. The thief stopped abruptly as the traveler bypassed a crowd of people, causing the traveler to also stop. A second thief, who was following close behind, quickly removed the traveler's laptop computer from his roll bag and disappeared into the crowd.

A traveler to Russia may have his laptop confiscated by the Russian Government. In 1998, two US Government contractors, working on a joint US-Russian project, had completed their task and were returning home. As they passed through Russian Customs, the official told one of the contractors that they would have to surrender their laptops to Russian authorities. When the contractors protested, the Russian official said that Russian law requires the laptop computers to

be examined 48 hours before leaving the country to determine if any Russian "secrets" were being smuggled out of the country. This is the only time of which the US Government is aware that the Russians have used a catchall paragraph in their law to retain a laptop. Letters were sent requesting the return of the laptops, and they were returned six months later.

At Orly Airport in Paris, a US Government contractor had his laptop stolen from an airport bus as he was transferring from one airport gate to another after a change in his flight. The contractor had taken all precautions to guard his laptop while in France until he boarded the bus. Thinking he was safe, he placed his laptop with his other bags on the luggage rack. When he went to retrieve it, the laptop was gone.

In late October 2000, Julien Holstein, information security director at Airbus, warned travelers not to work on company-sensitive projects on laptop computers while flying. During his talk at the Computer Security, Audit, and Control conference in London, Holstein said his firm introduced a companywide policy forbidding Airbus staff to work on projects using their laptops when flying on business. The policy had been introduced "to maintain the integrity of the company's data after one of its managers reported that he had covertly read sensitive project information off the laptop screen of the person in the next seat."¹

At the Department of State, a laptop that contained thousands of pages of highly classified information disappeared on 20 January 2000 from an allegedly secure workspace in the Office of Strategic Proliferation and Military Affairs in the Bureau of Intelligence and Research. It has yet to be recovered. An inventory at State Department headquarters in Washington confirmed that 15 out of 1,913 unclassified laptop computers are missing. "It's possible they were stolen," a spokesman said. "Some could be lost." Only one classified computer is missing so far, and department officials still aren't sure if espionage was involved.

The FBI is investigating whether the theft of a laptop owned by Qualcomm's CEO Irwin Jacobs was the work of thieves or an act of economic espionage. After speaking to members of the Society of American Business Editors and Writers at the Hyatt-Regency in Irvine, California, in September 2000, the CEO went over to speak to a small group of attendees. When he returned 15 to 20 minutes later, his IBM Think-Pad laptop—worth about \$4,000—was gone. The CEO said that the laptop contained proprietary information that could be valuable to foreign governments.

The FBI is not exempt from losing laptops. Conducting an internal inventory, the FBI discovered that 184 laptop computers, including at least one containing classified data, were missing or perhaps stolen. The secret data on the laptop concerned two closed cases. Bureau officials also said three other missing computers were suspected of containing classified information.

The loss of classified US Government information and US proprietary information is not limited to laptop thefts in the United States. In Canada, Ottawa businesses and institutions reported that \$6.7 million of computer equipment was stolen in 1997.²

In May 2000, a laptop was taken from a British naval intelligence officer as he sat on a train at London's Paddington Station. The laptop contained top secret information on the supersonic Anglo-US Strikefighter. After being stolen, the computer passed through a number of hands. It came into *The Mirror's* (a British newspaper) possession after a computer specialist who said that a contact wanted him to wipe a laptop of "fighter plane stuff" contacted the paper. *The Mirror*, which bought a new machine and switched laptops without the original contact being aware, returned the laptop to the British Government. A relieved military expert said, "It is unbelievable it could be stolen apparently so easily."

The above laptop was stolen from the same rail station where, two months previously, an MI5 officer (British internal security service) had his

laptop stolen when he put it down to buy a ticket. Just a few days later, a laptop was mislaid by an MI6 (British foreign intelligence) officer who had been drinking at a tapas bar near MI6's South London headquarters. It is thought that he left it in a taxi on the way home. The officer did not realize it was missing until the next day. In April 1999, an Army officer had a laptop stolen at Heathrow Airport. A portable PC belonging to a British Royal Navy Commander was later taken from a car in Pinner, Middlesex. The computer, which contained top secret and classified material, was not password protected.

It appears that British media coverage of missing laptops has had no real affect on security practices because in April 2001 another British Ministry of Defense (MoD) official left his laptop containing top secret information in a taxi. According to the British press, the individual reported the missing laptop to the police station in Wandsworth, South London. The official informed the police that he had taken a cab near Waterloo railway station to Roehampton. When he got out of the taxi, he forgot about the laptop and left it in the cab. Police immediately alerted Scotland Yard's Special Branch. This is only the latest of a large number of computers that have gone missing through carelessness or theft—sometimes after drinking sessions

The Mirror reported that, since 1997, military and intelligence staffs have lost an astonishing 204 laptops containing official secrets. The problem is so serious that the MoD and security service staffs are to be issued hi-tech briefcases costing 1,000 pounds each. The MoD plans to buy 15,000 of the armoured cases that look like ordinary black briefcases but will destroy data if an unauthorized attempt is made to open them.

The Mirror, citing an MoD spokesperson, stated that the new briefcases are so strong that they can withstand a Semtex explosion. Special versions will have an electronic system that erases the laptop's hard drive if the case is opened without the right codes. The briefcases were recently displayed at a private security exhibition at the

MoD's Whitehall headquarters and were passed for use by a secretive Cabinet Office body called the Security Equipment Assessment Panel. Some of the briefcases will also be fitted with electronic trackers so that they can be traced quickly if they are misplaced.³

If your company's security is not adequate, thieves can enter your office and steal proprietary information. Consider the case of John Labatt Ltd., whose offices were entered by a thief who stole five laptop computers. The physical security at Labatt in the heart of Toronto's financial district was easily breached. Espionage is suspected because the thief ignored cash and other valuables. Labatt is being eyed by at least two suitors for a hostile takeover so that any private information would be of much greater value on the street than just the physical worth of the laptops.

A laptop is not immune from theft in a hotel. Some countries convince hotel operators to provide intelligence collectors with access to visitors' luggage or rooms. During these surreptitious break-ins, known colloquially as "bag ops," unattended luggage is searched for sensitive information, and any useful documents are copied or simply stolen.

Economic and industrial espionage may involve simply breaking into a hotel room or an office containing desired information. Break-ins at the foreign offices of American companies have resulted in the theft of laptop computers and/or disks even when more valuable items are in the vicinity. These instances are not always reported, or they are reported as merely break-ins, without considering the possibility that the target was information rather than equipment.

In another example, a major US consumer products company suffered a possible loss of proprietary information as a result of a theft in East Asia. A laptop computer containing sales data, market estimates, and strategic business plans for one of its business units was stolen from a hotel conference room during a lunch break. Hotel staff—under the supervision of a company employee who was preparing remarks for the next presentation—

cleaned the room for the afternoon session. The employee did not continuously guard the computer and discovered the loss shortly before the session reconvened.

When a laptop is stolen, one doesn't know whether it was taken for the value of the information on the computer or for the value of the computer itself. This makes it difficult to assess the damage caused by the loss. In addition, stolen laptops are rarely recovered mainly because it is difficult to prove ownership if the owner did not bother to record the laptop's serial number.

Endnotes

¹ Lynch, Ian. "Laptop secrets not safe on planes." *NewMonday.com*, 3 November 2000.

² *Monitor Magazine*, April 1997.

³ "The Laptop Shambles." *The Mirror*, 16 April 2001.

The Presidential Decision Directive on CI-21: Counterintelligence for the 21st Century

The White House released the following on 6 January 2001:

FACT SHEET

President Clinton signed a Presidential Decision Directive (PDD) entitled “U.S. Counterintelligence Effectiveness—Counterintelligence for the 21st Century.” The PDD outlines specific steps that will enable the U.S. counterintelligence (CI) community to better fulfill its mission of identifying, understanding, prioritizing and counteracting the intelligence threats faced by the United States. The system will be predictive, proactive and will provide integrated oversight of counterintelligence issues across the national security agencies.

Specifically, the PDD directs the following structure be established to continue the task of improving U.S. counterintelligence effectiveness:

Counterintelligence Board of Directors

- A National Counterintelligence Board of Directors, chaired by the Director, FBI and composed of the Deputy Secretary of Defense, Deputy Director of Central Intelligence and a senior representative of the Department of Justice is hereby established.
- The Board, chaired by the Director of the FBI, will operate by consensus, and will select, oversee and evaluate the National Counterintelligence Executive (CI Executive) and will promulgate the mission, role and responsibilities of the CI Executive.
- The Board will approve the National Counterintelligence Strategy drawn from the annual National Threat Identification and Prioritization Assessment, ensuring the integration of government and private sector interests.

- The Board working with Congress, OMB, and other Executive Branch agencies will ensure the CI Executive has adequate resources to carry out his/her responsibilities and duties.

NSC Deputies Committee

- The NSC Deputies Committee, to include the Director of the FBI, will review the annual National Threat Identification and Prioritization Assessment and will meet at least semiannually, to review progress in implementing the National Counterintelligence Strategy.
- The Deputies Committee will ensure that the strategy, priorities and activities of the CI Community are grounded in national policy goals and objectives; the Deputies Committee shall also ensure that CI analysis and information is provided to assist national policy deliberations as appropriate. The Board of Directors through the CI Executive will be responsible for ensuring the implementation of these decisions.

The National Counterintelligence Executive

- The position of CI Executive is established and empowered to execute certain responsibilities on behalf of the Board of Directors and will serve as the substantive leader of national-level counterintelligence. The CI Executive will be a federal employee, selected by the Board of Directors with the concurrence of the Attorney General, DCI and the Secretary of Defense.
- The CI Executive will report to the FBI Director, as Chairman of the Board of Directors, but will be responsible to the Board of Directors as a whole. The Board will, through the Chairman, oversee and evaluate the CI Executive.
- The CI Executive and the National Coordinator for Security, Infrastructure Protection and Counterterrorism will work together to insure that both of their programs are well coordinated with each other.

-
- The CI Executive, in carrying out the duties and responsibilities of the position, will advise members of the Board on counterintelligence programs and policies.

The National Counterintelligence Policy Board

- The CI Executive will chair the National Counterintelligence Policy Board. Senior counterintelligence officials from State, Defense, Justice, Energy, JCS, CIA, FBI and NSC Staff, at a minimum will serve on the Policy Board. The NSC Deputies Committee will approve the composition, functions and duties of the Policy Board, which will be consistent with the statutorily defined functions of the Policy Board. The Policy Board will establish, with the approval of the Board of Directors, other interagency boards and working groups as necessary.
- The Policy Board, under the chairmanship of the CI Executive, will serve as an Interagency Working Group to prepare issues relating to the full implementation of this PDD for Deputies discussions and review, as well as a forum to provide advice to the CI Executive on priorities with respect to the National Counterintelligence Strategy.

Office of the CI Executive

- The CI Executive, on behalf of the Board of Directors, will head the Office of the National Counterintelligence Executive, which will among its other functions assume the functions previously exercised by the NACIC. To the extent permitted by law, resources previously assigned to the NACIC will become the initial resource base for the Office of the CI Executive. The Office will develop and deploy the following capabilities:

National CI Strategic Planning

- The Office, in consultation with United States government agencies and the private sector, will produce an annual report entitled The National Threat Identification and Prioritization Assessment for review by the Deputies Committee.
- The Office, drawing on this Assessment and working with the policy community, appropriate Government counterintelligence organizations and the private sector, will formulate and, subject to the approval of the Board of Directors, publish the National Counterintelligence Strategy.

National CI Strategic Analysis

- The Office will oversee and coordinate the production of strategic national CI analysis and will be supported in this endeavor by all components of the Executive Branch.
- The Office will oversee and coordinate the production of CI damage assessments and “lessons learned” papers with full support from Executive Branch components.

National CI Program Budget and Evaluation

- The Office, working with the DCI’s Community Management Staff, will review, evaluate, and coordinate the integration of CI budget and resource plans of, initially, the DOD, CIA and FBI. It will report to the Board of Directors and the Deputies Committee on how those plans meet the objectives and priorities of the National CI Strategy.

-
- The Office will evaluate the implementation of the National CI Strategy by the CI community agencies and report to the Board of Directors and Deputies Committee. The Office will also identify shortfalls, gaps and weaknesses in agency programs and recommend remedies.

National CI Collection and Targeting Coordination

- The Office will develop for approval by the Board of Directors strategic CI investigative, operational and collection objectives and priorities that implement the National CI Strategy.
- The Office will not have an operational role in CI operations and investigations and no independent contacts or activities with foreign intelligence services.

National CI Outreach, Watch and Warning Capability

- The Office will conduct and coordinate CI vulnerability surveys throughout government, and with the private sector as appropriate, while working with the Security Policy community. It will engage government and private sector entities to identify more clearly and completely what must be protected.
- The Office will conduct and coordinate CI community outreach programs in the government and private sector. It will serve as the national coordination mechanism for issuing warnings of counterintelligence threats to the national security.
- The Office will work with various government and private sector R&D centers to explore technology needs and solutions for the CI community. The Office will ensure that emerging technology and products and services are used effectively.

In addition, the Office will develop policies for CI training and professional development for CI investigators, operators, and analysts. It will also develop and manage joint training exercises, and assess the need for a National CI Training Academy. Also, the CI Executive and the Office will have a Principal Legal Advisor who will ensure that all activities of the Executive and the office comport with the law, Executive Orders and Attorney General Guidelines. The Principal Legal Advisor will provide advice and counsel to the Executive and the Office regarding national security law issues. The Advisor will coordinate with the appropriate law enforcement, intelligence and defense agencies' General Counsels and Legal Advisors in providing legal advice, guidance and representation to the Executive and the Office.

National Security Presidential Directive-1

(Editor's Note: President George W. Bush decided that the directives used to promulgate Presidential decisions on national security matters would be designated National Security Presidential Directives [NSPDs]. This new category of directives supersedes both the Presidential Decision Directives and the Presidential Review Directives of the Clinton Administration.)

SUBJECT: Organization of the National Security Council System

This document is the first in a series of National Security Presidential Directives. National Security Presidential Directives shall replace both Presidential Decision Directives and Presidential Review Directives as an instrument for communicating presidential decisions about the national security policies of the United States.

National security includes the defense of the United States of America, protection of our constitutional system of government, and the advancement of United States interests around the globe. National security also depends on America's opportunity to prosper in the world economy. The National Security Act of 1947, as amended, established the National Security Council to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. That remains its purpose. The NSC shall advise and assist me in integrating all aspects of national security policy as it affects the United States - domestic, foreign, military, intelligence, and economics (in conjunction with the National Economic Council (NEC)). The National Security Council system is a process to coordinate executive departments and agencies in the effective development and implementation of those national security policies.

The National Security Council (NSC) shall have as its regular attendees (both statutory and non-statutory) the President, the Vice President, the Secretary of State, the Secretary of the Treasury,

the Secretary of Defense, and the Assistant to the President for National Security Affairs. The Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff, as statutory advisors to the NSC, shall also attend NSC meetings. The Chief of Staff to the President and the Assistant to the President for Economic Policy are invited to attend any NSC meeting. The Counsel to the President shall be consulted regarding the agenda of NSC meetings, and shall attend any meeting when, in consultation with the Assistant to the President for National Security Affairs, he deems it appropriate. The Attorney General and the Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities. For the Attorney General, this includes both those matters within the Justice Department's jurisdiction and those matters implicating the Attorney General's responsibility under 28 U.S.C. 511 to give his advice and opinion on questions of law when required by the President. The heads of other executive departments and agencies, as well as other senior officials, shall be invited to attend meetings of the NSC when appropriate.

The NSC shall meet at my direction. When I am absent from a meeting of the NSC, at my direction the Vice President may preside. The Assistant to the President for National Security Affairs shall be responsible, at my direction and in consultation with the other regular attendees of the NSC, for determining the agenda, ensuring that necessary papers are prepared, and recording NSC actions and Presidential decisions. When international economic issues are on the agenda of the NSC, the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy shall perform these tasks in concert.

The NSC Principals Committee (NSC/PC) will continue to be the senior interagency forum for consideration of policy issues affecting national security, as it has since 1989. The NSC/PC shall have as its regular attendees the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Chief of Staff to the President, and the Assistant to the President for National Security Affairs (who shall serve as chair). The Director

of Central Intelligence and the Chairman of the Joint Chiefs of Staff shall attend where issues pertaining to their responsibilities and expertise are to be discussed. The Attorney General and the Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities. For the Attorney General, this includes both those matters within the Justice Department's jurisdiction and those matters implicating the Attorney General's responsibility under 28 U.S.C. 511 to give his advice and opinion on questions of law when required by the President. The Counsel to the President shall be consulted regarding the agenda of NSC/PC meetings, and shall attend any meeting when, in consultation with the Assistant to the President for National Security Affairs, he deems it appropriate. When international economic issues are on the agenda of the NSC/PC, the Committee's regular attendees will include the Secretary of Commerce, the United States Trade Representative, the Assistant to the President for Economic Policy (who shall serve as chair for agenda items that principally pertain to international economics), and, when the issues pertain to her responsibilities, the Secretary of Agriculture. The Chief of Staff and National Security Adviser to the Vice President shall attend all meetings of the NSC/PC, as shall the Assistant to the President and Deputy National Security Advisor (who shall serve as Executive Secretary of the NSC/PC). Other heads of departments and agencies, along with additional senior officials, shall be invited where appropriate.

The NSC/PC shall meet at the call of the Assistant to the President for National Security Affairs, in consultation with the regular attendees of the NSC/PC. The Assistant to the President for National Security Affairs shall determine the agenda in consultation with the foregoing, and ensure that necessary papers are prepared. When international economic issues are on the agenda of the NSC/PC, the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy shall perform these tasks in concert.

The NSC Deputies Committee (NSC/DC) will also continue to serve as the senior sub-Cabinet

interagency forum for consideration of policy issues affecting national security. The NSC/DC can prescribe and review the work of the NSC interagency groups discussed later in this directive. The NSC/DC shall also help ensure that issues being brought before the NSC/PC or the NSC have been properly analyzed and prepared for decision. The NSC/DC shall have as its regular members the Deputy Secretary of State or Under Secretary of the Treasury or Under Secretary of the Treasury for International Affairs, the Deputy Secretary of Defense or Under Secretary of Defense for Policy, the Deputy Attorney General, the Deputy Director of the Office of Management and Budget, the Deputy Director of Central Intelligence, the Vice Chairman of the Joint Chiefs of Staff, the Deputy Chief of Staff to the President for Policy, the Chief of Staff and National Security Adviser to the Vice President, the Deputy Assistant to the President for International Economic Affairs, and the Assistant to the President and Deputy National Security Advisor (who shall serve as chair). When international economic issues are on the agenda, the NSC/DC's regular membership will include the Deputy Secretary of Commerce, a Deputy United States Trade Representative, and, when the issues pertain to his responsibilities, the Deputy Secretary of Agriculture, and the NSC/DC shall be chaired by the Deputy Assistant to the President for International Economic Affairs for agenda items that principally pertain to international economics. Other senior officials shall be invited where appropriate.

The NSC/DC shall meet at the call of its chair, in consultation with the other regular members of the NSC/DC. Any regular member of the NSC/DC may also request a meeting of the Committee for prompt crisis management. For all meetings the chair shall determine the agenda in consultation with the foregoing, and ensure that necessary papers are prepared.

The Vice President and I may attend any and all meetings of any entity established by or under this directive.

Management of the development and implementation of national security policies by multiple agencies of the United States Government shall usually be accomplished by the NSC Policy Coordination Committees (NSC/PCCs). The NSC/PCCs shall be the main day-to-day fora for interagency coordination of national security policy. They shall provide policy analysis for consideration by the more senior committees of the NSC system and ensure timely responses to decisions made by the President. Each NSC/PCC shall include representatives from the executive departments, offices, and agencies represented in the NSC/DC.

Six NSC/PCCs are hereby established for the following regions: Europe and Eurasia, Western Hemisphere, East Asia, South Asia, Near East and North Africa, and Africa. Each of the NSC/PCCs shall be chaired by an official of Under Secretary or Assistant Secretary rank to be designated by the Secretary of State.

Eleven NSC/PCCs are hereby also established for the following functional topics, each to be chaired by a person of Under Secretary or Assistant Secretary rank designated by the indicated authority:

Democracy, Human Rights, and International Operations (by the Assistant to the President for National Security Affairs);

International Development and Humanitarian Assistance (by the Secretary of State);

Global Environment (by the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy in concert);

International Finance (by the Secretary of the Treasury);

Transnational Economic Issues (by the Assistant to the President for Economic Policy);

Counter-Terrorism and National Preparedness (by the Assistant to the President for National Security Affairs);

Defense Strategy, Force Structure, and Planning (by the Secretary of Defense);

Arms Control (by the Assistant to the President for National Security Affairs);

Proliferation, Counterproliferation, and Homeland Defense (by the Assistant to the President for National Security Affairs);

Intelligence and Counterintelligence (by the Assistant to the President for National Security Affairs); and

Records Access and Information Security (by the Assistant to the President for National Security Affairs).

The Trade Policy Review Group (TPRG) will continue to function as an interagency coordinator of trade policy. Issues considered within the TPRG, as with the PCCs, will flow through the NSC and/or NEC process, as appropriate.

Each NSC/PCC shall also have an Executive Secretary from the staff of the NSC, to be designated by the Assistant to the President for National Security Affairs. The Executive Secretary shall assist the Chairman in scheduling the meetings of the NSC/PCC, determining the agenda, recording the actions taken and tasks assigned, and ensuring timely responses to the central policymaking committees of the NSC system. The Chairman of each NSC/PCC, in consultation with the Executive Secretary, may invite representatives of other executive departments and agencies to attend meetings of the NSC/PCC where appropriate.

The Assistant to the President for National Security Affairs, at my direction and in consultation with the Vice President and the Secretaries of State, Treasury, and Defense, may establish additional NSC/PCCs as appropriate.

The Chairman of each NSC/PCC, with the agreement of the Executive Secretary, may establish subordinate working groups to assist the PCC in the performance of its duties.

The existing system of Interagency Working Groups is abolished.

The oversight of ongoing operations assigned in PDD/NSC-56 to Executive Committees of the Deputies Committee will be performed by the appropriate regional NSC/PCCs, which may create subordinate working groups to provide coordination for ongoing operations.

The Counter-Terrorism Security Group, Critical Infrastructure Coordination Group, Weapons of Mass Destruction Preparedness, Consequences Management and Protection Group, and the interagency working group on Enduring Constitutional Government are reconstituted as various forms of the NSC/PCC on Counter-Terrorism and National Preparedness.

The duties assigned in PDD/NSC-75 to the National Counterintelligence Policy Group will be performed in the NSC/PCC on Intelligence and Counterintelligence, meeting with appropriate attendees.

The duties assigned to the Security Policy Board and other entities established in PDD/NSC-29 will be transferred to various NSC/PCCs, depending on the particular security problem being addressed.

The duties assigned in PDD/NSC-41 to the Standing Committee on Nonproliferation will be transferred to the PCC on Proliferation, Counterproliferation, and Homeland Defense.

The duties assigned in PDD/NSC-35 to the Interagency Working Group for Intelligence Priorities will be transferred to the PCC on Intelligence and Counterintelligence.

The duties of the Human Rights Treaties Interagency Working Group established in E.O. 13107 are transferred to the PCC on Democracy,

Human Rights, and International Operations. The Nazi War Criminal Records Interagency Working Group established in E.O. 13110 shall be reconstituted, under the terms of that order and until its work ends in January 2002, as a Working Group of the NSC/PCC for Records Access and Information Security.

Except for those established by statute, other existing NSC interagency groups, ad hoc bodies, and executive committees are also abolished as of March 1, 2001, unless they are specifically reestablished as subordinate working groups within the new NSC system as of that date. Cabinet officers, the heads of other executive agencies, and the directors of offices within the Executive Office of the President shall advise the Assistant to the President for National Security Affairs of those specific NSC interagency groups chaired by their respective departments or agencies that are either mandated by statute or are otherwise of sufficient importance and vitality as to warrant being reestablished. In each case the Cabinet officer, agency head, or office director should describe the scope of the activities proposed for or now carried out by the interagency group, the relevant statutory mandate if any, and the particular NSC/PCC that should coordinate this work. The Trade Promotion Coordinating Committee established in E.O. 12870 shall continue its work, however, in the manner specified in that order. As to those committees expressly established in the National Security Act, the NSC/PC and/or NSC/DC shall serve as those committees and perform the functions assigned to those committees by the Act.

To further clarify responsibilities and effective accountability within the NSC system, those positions relating to foreign policy that are designated as special presidential emissaries, special envoys for the President, senior advisors to the President and the Secretary of State, and special advisors to the President and the Secretary of State are also abolished as of March 1, 2001, unless they are specifically redesignated or reestablished by the Secretary of State as positions in that Department.

This Directive shall supersede all other existing presidential guidance on the organization of the National Security Council system. With regard to application of this document to economic matters, this document shall be interpreted in concert with any Executive Order governing the National Economic Council and with presidential decision documents signed hereafter that implement either this directive or that Executive Order.

[signed: George W. Bush]

cc: The Executive Clerk

Bibliography Volume IV

Aldrich, Richard J. *Intelligence and the War Against Japan: Britain, America and the Politics of Secret Service*. Cambridge University Press, Cambridge, UK, 2000.

Espionage, Security and Intelligence in Britain 1945-1970. Manchester University Press, Manchester, UK, 1998.

Allen, George W. *None So Blind: A Personal Account of the Intelligence Failure in Vietnam*. Ivan R. Dee, Inc., Chicago, IL, 2001.

Alvarez, David. *Secret Messages: Codebreaking and American Diplomacy: 1930-1945*. University Press of Kansas, Lawrence, KS, 2000.

Andrew, Christopher and Vasili Mitrokhin. *The Sword and The Shield: The Mitrokhin Archive and the Secret History of the KGB*. Basic Books, New York, NY, 1999.

Bath, Alan Harris. *Tracking the Axis Enemy: The Triumph of Anglo-American Naval Intelligence*. University Press of Kansas, Lawrence, KS, 1998.

Bamford, James. *Body of Secrets: Anatomy of the Ultra Secret National Security Agency*. Doubleday, New York, NY, 2001.

Beesly, Patrick. *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre, 1939-1945*. Greenhill Books/Lionel Levanthal, London, UK, 2000.

Berkowitz, Bruce D. and Allan E. Goodman. *Best Truth: Intelligence in the Information Age*. Yale University Press, New Haven, CT, 2000.

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II*. Free Press, New York, NY, 2000.

Burrows, William E. *By Any Means Necessary: America's Secret Air War in the Cold War*. Farrar, Straus & Giroux, New York, NY, 2001.

Cole, D.S. *Geoffrey Prime: The Imperfect Spy*. Robert Hale Ltd, London, UK, 2001.

Conboy, Kenneth and Dale Andrade. *Spies and Commandos: How America Lost the Secret War in North Vietnam*. University Press of Kansas, Lawrence, KS, 2000.

Conboy, Kenneth and James Morrison. *Feet to the Fire: CIA Covert Operations in Indonesia, 1957-1958*. Naval Institute Press, Annapolis, MD, 2000.

Daugherty, William J. *In the Shadow of the Ayatollah: A CIA Hostage in Iran*. Naval Institute Press, Annapolis, MD, 2001.

Day, Dwayne A, ed. *Eye in the Sky: The Story of the Corona Spy Satellites*. Smithsonian Institution Press, Washington, D.C., 1998.

de Graffenreid, Kenneth, ed. *The Cox Report*. Regnery Publishing, Washington, DC, 1999.

Dorril, Stephen, MI: *Inside the Covert World of Her Majesty's Secret Intelligence Service*. The Free Press, New York, NY, 2000.

Doyle, David W. *True Men and Traitors: From the OSS to the CIA, My Life in the Shadows*, John Wiley & Sons, New York, NY, 2001.

Duff, William E. *A Time for Spies: Theodore Stephanovich Mally and the Era of the Great Illegals*. Vanderbilt University Press, Nashville, TN, 1999.

Douglas, Hugh. *Jacobite Spy Wars: Moles, Rogues and Treachery*. Sutton Publishing, Phoenix Mill, UK, 1999.

Eisendrath, Craig R., ed. *National Insecurity: US Intelligence After the Cold War*. Temple University Press, Philadelphia, PA, 1999.

Feklisov, Alexander and Sergei Kostin. *The Man Behind the Rosenbergs*. Enigma Books, New York, NY, 2001.

Gannon, James. *Stealing Secrets, Telling Lies: How Spies & Codebreakers Helped Shape the Twentieth Century*. Brassey's Inc., New York, NY, 2001.

Gertz, Bill. *Betrayal*. Regnery Publishing Inc., Washington, DC, 1999.

Gibson, Steve. *The Last Mission: Behind the Iron Curtain*. Sutton Publishing, Phoenix Mill, UK, 1998.

Goldenberg, Elliot and Alan Dershowitz. *The Hunting Horse: The Truth Behind the Jonathan Pollard Spy Case*. Prometheus Books, Amhurst, NY, 2000.

Golitt, Leslie. *Spy Master, The Real-Life Karla, His Moles and the East German Secret Police*. Addison-Wesley Publishing Co., Reading, MA, 1995.

Gross, Peter. *Operation Rollback: America's Secret War behind the Iron Curtain*. Houghton Mifflin Co., Boston, MA, 2000.

Gudgin, Peter. *Military Intelligence: A History*. Sutton Publishing, Phoenix Mill, UK, 2000.

Gup, Ted. *The Book of Honor Covert Lives and Classified Deaths at the CIA*. Random House, New York, NY, 2000.

Harvill, Adrian. *The Spy Who Stayed Out in the Cold: The Secret Life of FBI Double Agent Robert Hanssen*. St. Martin's Press, New York, NY, 2001.

Haynes, John Earl and Harvey Klehr. *Venona: Decoding Soviet Espionage in America*. Yale University Press, New Haven, CT, 1999.

Herrington, Stuart A. *Traitors Among US, Inside the Spy Catcher's World*. Presidio Press, Novato, CA, 1999.

Holobar, Frank. *Raiders of the China Coast: CIA Covert Operations during the Korean War*. Naval Institute Press, Annapolis, MD, 1999.

Hunter, Robert W. *Spy Hunter: Inside the FBI Investigation of the Walker Espionage Case*. Naval Institute Press, Annapolis, MD, 1999.

Jackson, Robert. *High Cold War: Strategic Air Reconnaissance and the Electronics Intelligence War*. Patrick Stephens Limited, Somerset, UK, 1998.

Jakub, Jay and D. Phil. *Spies and Saboteurs: Anglo-American Collaboration and Rivalry in Human Intelligence Collection and Special Operations 1940-1945*. Palgrave, Basingstoke, UK, 1999.

Jeffreys-Jones, Rhodri. *The CIA and American Democracy*. Yale University Press, New Haven, CT, 1998.

Knight, Amy. *Spies Without Cloaks, The KGB's Successors*. Princeton University Press, Princeton, NJ, 1996.

Kornbluh, Peter, ed. *Bay of Pigs Declassified, The Secret CIA Report on the Invasion of Cuba*. The New Press, New York, NY, 1998.

Krivitsky, W.G., Sam Tanenhaus, and Santi Corvaja. *In Stalin's Secret Service: Memoirs of the First Soviet Master Spy to Defect*. Enigma Books, New York, NY, 2000.

Lamont-Brown, Raymond. *Kampeitai: Japan's Dreaded Military Police*. Sutton Publishing, Phoenix Mill, UK, 1998.

Leonard, Raymond W. *Secret Soldiers of the Revolution: Soviet Military Intelligence, 1918-1933*. Greenwood Publishing, Westport, CT, 2000.

Lindgren, David T. *Trust but Verify: Imagery Analysis in the Cold War*. Naval Institute Press, Annapolis, MD, 2000.

Lunev, Stanislav and Ira Winkler. *Through the Eyes of the Enemy: Russia's Highest Ranking Military Defector Reveals Why Russia Is More Dangerous Than Ever*. Regnery Publishing, Washington, DC, 1998.

Macdonald, Bill J. *The True 'Intrepid': Sir William Stephenson and the Unknown Agents*. Timberholme Books, Surry, British Columbia, Canada, 1998.

Maffeo, Steven E. *Most Secret and Confidential: Intelligence in the Age of Nelson*. Naval Institute Press, Annapolis, MD, 2000.

Mahl, Thomas E. *Desperate Deception: British Covert Operations in the United States, 1939-44*. Brassey's, New York, NY, 1998.

Marks, Leo. *Between Silk and Cyanide, A Codemaker's War 1941-1945*. Free Press, New York, NY, 1998.

Masetti, Jorge. *In the Pirate's Den: My Life as a Secret Agent for Castro*. Encounter Books, San Francisco, CA, 2001.

Melton, Buckner F. *Aaron Burr: Conspiracy to Treason*. John Wiley & Sons, New York, NY, 2001.

Mitrovich, Gregory. *Undermining the Kremlin: America's Strategy to Subvert the Soviet Bloc 1947-1956*. Cornell University Press, Ithaca, NY, 2000.

Morgan, Ted. *A Covert Life: Jay Lovestone, Communist Anticommunist and Spymaster*. Random House, New York, NY, 1999.

Osborn, Shane and Malcolm McConnell. *Born to Fly: The Untold Story of the Downed American Reconnaissance Plane*, Broadway Books, New York, NY, 2001.

Perisco, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage*. Random House, New York, NY, 2001.

Polmar, Norman and Thomas B. Allen. *The Encyclopedia of Espionage*. Grammercy, New York, NY, 1998.

Richelson, Jeffrey T. *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*. Westview Press, Boulder, CO, 2001.

Rigden, Denis. *Kill the Fuhrer: Section X and Operation Foxley*. Sutton Publishing, Phoenix Mill, UK, 2000.

Romerstein, Herbert and Eric Breindel. *The Venona Secrets: Exposing Soviet Espionage and America's Traitors*. Regency Publishing, Washington, DC, 2000.

Roberts, Sam. *The Brother: The Untold Story of Atomic Spy David Greenglass and How He Sent His Sister Ethel Rosenberg to the Electric Chair*. Random House, New York, NY, 2001.

Rudgers, David F. *Creating the Secret State: The Origins of the Central Intelligence Agency, 1943-1947*. University of Kansas Press, Lawrence, KS, 2000.

Russell, Frank Santi. *Information Gathering in Classical Greece*. University of Michigan Press, Ann Arbor, MI, 2000.

Saunders, Frances Stonor. *The Cultural Cold War: The CIA and the World of Arts and Letters*. The New Press, New York, NY, 1999.

Sawyer, Ralph D. *The Tao of Spycraft: Intelligence Theory and Practice in Traditional China*. Westview Press, Boulder, CO, 1998.

Schecter, Jerold L. and Leona P. Schecter. *Sacred Secrets: How Soviet Intelligence Operations Changed*. Brassey's, Inc, New York, NY, 2002.

Seabag-Nibtefiore Hugh. *Enigma: The Battle for the Code*. John Wiley & Son, New York, NY, 2001.

Seaman, Mark. *Secret Agent's Handbook: The WW II Spy Manual of Devices, Disguises, Gadgets and Concealed Weapons*. The Lyons Press, New York, NY, 2001.

Shannon, Elaine and Ann Blackman. *The Spy Next Door*. Little, Brown, Boston, MA, 2002.

Shaw, Mark. *Miscarriage of Justice: The Jonathan Pollard Story*. Paragon House, St. Paul, MN, 2001.

Sheldon, Rose Mary. *Tinker, Tailor, Caesar, Spy: Espionage in Ancient Rome*. Frank Cass, Ltd., London, UK, 2001.

Shultz, Eichard H. Jr. *The Secret War Against Hanoi: Kennedy and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam*. Harper Collins, New York, NY, 1999.

Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. Doubleday, New York, NY, 1999.

Smith, Michael. *The Emperor's Codes, The Breaking of Japan's Secret Ciphers*. Arcade Publishing, New York, NY, 2000.

Spence, Jonathan D. *Treason by the Book*. Viking, New York, NY, 2001.

Srodes, James. *Allen Dulles Master of Spies*. Regnery Publishing, Washington, DC, 1999.

Stafford, David. *Secret Agent: the True Story of the Special Operations Executive*. Overlook Press, Woodstock, NY, 2001.

Roosevelt and Churchill, Men of Secrets. Overlook Press, Woodstock, NY, 2000.

Churchill and Secret Service. Overlook Press, Woodstock, NY, 1997.

Steele, Robert David. *On Intelligence: Spies and Secrecy in an Open World*. AFCEA International Press, Fairfax, VA, 2000.

Stephenson, William Samuel (editor) *British Security Coordination: The Secret History of British Intelligence in the Americas 1940-1945*, Fromm International Publishing Group, 1999.

Steury, Donald Paul and Roger Cirillo, eds. *The Intelligence War (World War II Chronicles)*. Metro Books, London, UK, 2000.

Stober, Dan and Ian Hoffman. *Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage*. Simon & Schuster, New York, NY, 2002.

Tart, Larry and Robert Keefe. *Attacks on American Surveillance Flights: The Price of Vigilance*. Ballantine Books, New York, NY, 2001.

Trento, Joseph J. *The Boys From Berlin: The Secret History of the CIA*. Roberts Rinehart Publishers, Niwot, CT, 1999.

The Secret History of the CIA, Prime Publishing. Highland Park, IL, 2001.

Tourison, Sedgwick. *Secret Army Secret War Washington's Tragic Spy Operation in North Vietnam*. Naval Institute Press, Annapolis, MD, 1995.

Vise, David A. *The Bureau and the Mole: The Unmasking of Robert Philip Hanssen, the Most Dangerous Double Agent in FBI History*. Atlantic Monthly Press, Atlanta, GA, 2002.

Von Rintelen, Franz. *The Dark Invader: Wartime Reminiscences of a German Naval Intelligence Officer*. Frank Cass & Co., London, UK, 1998.

Warner, Roger. *Back Fire: The CIA's Secret War in Laos and its Link to the War in Vietnam*. Simon and Schuster, New York, NY, 1995.

Wasserstein, Allen and Alexander Vassiliev. *The Haunted Wood*. Random House, New York, NY, 1999.

Wasserstein, Bernard. *Secret War in Shanghai*.

Houghton Mifflin Co, Boston, MA, 1999.

Weber, Ralph E., ed. *Spymasters: Ten CIA Officers in Their Own Words*, Tyndale House Publishers, Carol Stream, IL, 1998.

Wen Ho Lee. *My Country Versus Me*. Hyperion, New York, NY, 2001.

West, Nigel. *The Crown Jewels: The British Secrets at the Heart of the KGB Archives*. Yale University Press, New Haven, CT, 1999.

Whiting, Charles. *Hitler's Secret War: the Nazi Espionage Campaign Against the Allies*. Casemate Publishers, Haverton, PA, 2000.

Whymont, Robert. *Stalin's Spy: Richard Sorge and the Tokyo Espionage Ring*. St. Martin's Press, New York, NY, 1999.

Wires, Richard. *The Cicero Spy Affair: German Access to British Secrets in World War II*. Praeger Publishing Trade, Westport, CT, 1999.

Wise, David. *Cassidy's Run*. Random House, New York, NY, 2000.

CI Calendar of Events

7 January 1998

Clyde Lee Conrad, a former US Army Sergeant who was convicted of treason in 1990, dies in a German prison in January 1999, where he was serving a life sentence.

26 January 1998

Steven L. David pleads guilty to federal charges that he stole and disclosed Gillette Company trade secrets. He was sentenced on 17 April 1998 to 27 months in prison.

11 February 1998

President Clinton issues Presidential Decision Directive-61 (PDD-61), which orders DOE to establish a stronger counterintelligence program.

26 February 1998

Arkady N. Shevchenko, a former high-ranking Soviet diplomat who defected to the United States on 6 April 1978, dies of a heart attack.

3 April 1998

FBI arrests CIA employee Douglas Frederick Groat on charges of espionage.

13 April 1998

New York Times reveals a May 1997 classified Pentagon report that concluded Hughes and Loral gave critical data to China that notably improved the reliability of its nuclear missiles.

11 May 1998

Israel officially acknowledges for the first time that Jonathan Pollard was an Israeli agent.

3 June 1998

James Clark, a one-time campus radical and former US Army paralegal, pleads guilty to conspiracy to commit espionage.

15 June 1998

The French magazine *Le Point* reports that France systematically listens in on the telephone

conversations and cable traffic of many businesses based in the United States and other nations.

17 June 1998

Department of Defense declassifies its first reconnaissance satellite, which was launched shortly after the 1 May 1960 shootdown of Francis Gary Power's U-2 over the Soviet Union.

25 July 1998

Russian President Boris Yeltsin appoints Vladimir Putin, a former KGB officer, to head the Federal Security Service from Nikolai Kovalev.

27 July 1998

CIA employee Douglas Frederick Groat pleads guilty to one count of attempted extortion after a plea agreement.

28 July 1998

FBI arrests Huang Dao Pei—a Chinese-born naturalized US citizen—on charges that, from 1992 to 1995, he tried to steal trade secrets of a hepatitis C monitoring kit from Roche Diagnostics and sell them to China.

1 August 1998

Joel Barr—an American communist and friend of Julius and Ethel Rosenberg—who barely eluded the FBI before he could be arrested for espionage in 1950, dies of complications of diabetes in a hospital in Moscow.

12 September 1998

Three-year FBI and other US Government agencies' investigation culminates in the arrest of a Cuban illegals network in Miami, Florida.

25 September 1998

Former CIA officer Douglas Groat gets five years in prison after pleading guilty to one count of extortion in return for prosecutors dropping four espionage counts.

5 October 1998

DOE Secretary Bill Richardson selects Lawrence H. Sanchez to be Director of the Office of Intelligence.

13 October 1998

FBI arrests retired US Army intelligence analyst David Sheldon Boone, charging him with selling secrets to Moscow.

6 November 1988

Kelly Warren, a former US Army soldier who served in Germany from 1984 to 1988, pleads guilty to one count of conspiracy to commit espionage.

13 November 1998

DOE Secretary Bill Richardson submits CI Action Plan to National Security Council.

5 December 1998

James M. Clark is sentenced to 12 years and seven months in prison for spying for East Germany and other countries.

20 December 1998

David Boone pleads guilty to conspiracy to commit espionage and is sentenced on 26 February 1999 to 24 years and four months in prison.

4 January 1999

Cox Committee submits its classified report to the President, which includes 38 recommendations addressing issues related to export control and counterintelligence.

22 January 1999

Theresa Marie Squillacote and her husband, Kurt Alan Stand, are sentenced to 21 and 17 years in prison on spy charges, respectively.

South Korea changes name of its spy agency to National Intelligence Service, apparently to dispel the agency's former tarnished image as a political tool of repression.

5 February 1999

British Government names Richard Dearlove as new Secret Intelligence Service (MI-6) chief, effective 1 September 1999.

12 February 1999

Kelly Warren is sentenced to 25 years in prison

on charges that she spied for Hungary and Czechoslovakia. She was part of the Clyde Lee Conrad espionage ring in Europe.

4 March 1999

DOE CI Implementation Plan (per PDD-61) is issued to Laboratories.

8 March 1999

DOE fires Wen Ho Lee, a computer scientist at Los Alamos, for allegedly leaking sensitive nuclear information to China.

9 March 1999

Based on faulty CIA information, NATO forces mistakenly bomb the Chinese Embassy in Belgrade.

18 March 1999

President Clinton requests the President's Foreign Intelligence Advisory Board (PFIAB) to review security threat at DOE's nuclear weapons laboratories and measures taken to address that threat.

31 March 1999

Kai-Lo Hsu, technical director of Yuen Foong Paper Co., Ltd., in Taiwan, pleads guilty to conspiring to steal Taxol formula from Bristol-Myers Squibb.

26 April 1999

Pin Yin Yang and Hwei Chen "Sally" Yang are convicted under Economic Espionage Act of 1996 of stealing corporate secrets from Avery Dennison.

17 May 1999

Former Australian intelligence official Jean Wispleare is charged with attempted espionage for selling secrets to an undercover FBI agent posing as a foreign spy.

15 June 1999

PFIAB presents the "Rudman Report" to President Clinton, which states DOE is a dysfunctional bureaucracy incapable of reforming itself.

July 1999

Russia expels US diplomat amid hints the case involved spying.

1 July 1999

Viktor M. Chebrikov, former KGB chairman (1982-88), dies unexpectedly at age 76.

13 July 1999

New Zealand Prime Minister appoints senior diplomat Richard Woods to head Security Intelligence Service, effective 1 November 1999.

22 July 1999

China outlaws Falun Gong, a spiritual sect in China whose leader, Li Hongzhi, has lived in New York since he left China in 1998.

4 October 1999

US Supreme Court rejects appeal by Robert Kim, who is serving a nine-year sentence for spying for South Korea.

1 November 1999

Theodore Alvin Hall, who passed Atom bomb secrets to Soviets, dies of cancer in Cambridge, England.

5 November 1999

US Navy First Class Petty Officer Daniel M. King is arrested after failing a routine polygraph examination.

18 November 1999

Russia's FSB domestic security service charges nuclear scientists Igor Sutyagin at Moscow's prestigious USA and Canada Institute with high treason.

29 November 1999

US military charges US Navy code breaker Daniel King with selling data to Moscow.

30 November 1999

Russian security officials advise catching Cheri Leberknight, a second secretary in the political section of the US Embassy, in the act of spying.

3 December 1999

President Clinton signs legislation, which creates an independent Agency for Nuclear Stewardship within DOE with authority for DOE's national security programs and nuclear weapons laboratories and production facilities.

8 December 1999

United States expels Stanislav Gusev, a Russian diplomat accused of monitoring a listening device planted in a State Department conference room.

10 December 1999

Wen Ho Lee, former DOE physicist, is indicted on 59 felony counts of mishandling national security information.

16 December 1999

United States and China reach agreement on compensation for damages arising out of accidental NATO bombing of the Chinese Embassy in Belgrade.

5 January 2000

P. Y. Yang of Taiwan-based Four Pillars, Ltd., is sentenced to two-years probation and six-months home detention for violating the 1996 Economic Espionage Act.

20 January 2000

Laptop containing thousands of pages of classified information disappears from State Department.

17 February 2000

Immigration and Naturalization Service employee Mariano Faget is arrested for espionage.

8 March 2000

Clinton Administration releases Unclassified version of an annual report on Chinese espionage in the United States.

8 March 2000

DCI, the FBI Director, and the Deputy Secretary of Defense unveil Counterintelligence *for the 21st Century* during a SSCI closed hearing. CI 21 restates and expands upon other recent assessments of the emerging CI environment.

17 March 2000

Armed Forces Court of Appeals suspends grand jury hearings in the case of accused spy Daniel King.

5 April 2000

Russian Federal Security Bureau detains retired US Navy intelligence officer, Edmond Pope, and a Russian accomplice for suspected espionage.

8 April 2000

US files espionage charges against Timothy Steven Smith, a civilian Defense Department employee assigned as an ordinary seaman aboard the USNS Kilauea, an ammunition ship.

14 June 2000

George Trofimoff, a retired Army colonel, is arrested and accused of spying for the Soviet Union in a 25-year-long Cold War conspiracy.

28 June 2000

Gen. John A. Gordon begins tenure as DOE Administrator of the National Nuclear Security Administration.

5 July 2000

European Parliament votes to investigate allegations that US using its surveillance apparatus, known as Echelon, to win commercial advantage for US companies.

7 July 2000

Ruth Werner, a communist spy who smuggled atom bomb secrets from Britain to the Soviet Union in the 1940s, dies at age 93.

9 August 2000

State Department offers \$25,000 for return of missing laptop containing classified information.

13 August 2000

Federal appeals court upheld espionage conviction of Theresa Marie Squillicote and Kurt Alan Stand.

8 September 2000

Shigehiro Hagisaki, Japan Maritime Defense Force, is arrested after passing a classified document to

Russian GRU official Capt. Viktor Bogatenkov.

13 September 2000

Wen Ho Lee pleads guilty to one count of mishandling classified information and sentenced to time served.

27 September 2000

Russian prosecutors charge Edmund Pope with espionage.

28 September 2000

State Department announces suspension of security clearances for five employees for security violations.

13 October 2000

Gus Hall, longtime Communist Party leader in the United States, dies.

16 October 2000

NSA Director Lt. Gen. Michael V. Hayden announces major reorganization to let senior managers focus on reengineering SIGINT to handle major advances in communications technologies.

23 October 2000

Romania's Supreme Court annuls former diplomat Mircea Raceanu's death sentence, acquitting him of charges of passing state secrets to the United States during the Communist era.

4 November 2000

President Clinton vetoes 2001 Intelligence Authorization Act, which has provision allowing easier prosecution of US officials leaking classified information.

14 November 2000

National Commission for the Review of the NRO recommends creation of an Office of Space Reconnaissance to pursue innovative technology for spying from space.

27 November 2000

Shigehiro Hagisaki pleads guilty to passing defense secrets, including information on US Navy units in Japan to Russian military attache.

6 December 2000

Edmond Pope, sentenced to 20 years in prison, becomes first American convicted of espionage in Russia since U-2 pilot Francis Gary Powers in 1960.

15 December 2000

Russian President Vladimir Putin pardons Edmond Pope, who returns to the United States.

17 December 2000

Press reports President Clinton faces new round of lobbying for release of Jonathan Pollard, who spied for Israel; however, Clinton leaves office without granting the pardon.

26 December 2000

Russia admits that the KGB murdered Swedish diplomat Raoul Wallenberg, who saved thousands of Jews in Nazi occupied Hungary during WWII.

4 January 2001

President Clinton signs Presidential Decision Directive (PDD)-75 creating National Counterintelligence Executive, replacing NACIC.

12 January 2001

Vladimir Semichastny, KGB chief from 1961 to 1967, dies in Moscow at age 78.

18 January 2001

FBI ends investigation of two missing hard drives at Los Alamos National Laboratories without finding any evidence of espionage.

20 January 2001

President Clinton pardons former US Navy intelligence analyst Samuel L. Morrison, the government official ever convicted to leaking classified information.

1 February 2001

Russian FSB arrests John Edward Tobin on drug charges but says he is part of the US intelligence establishment.

11 February 2001

Chinese authorities detain Gao Zhan—a Chinese

scholar working at American University—her husband, and 5-year-old son.

16 February 2001

Former DOE Secretary Bill Richardson temporarily suspends measures, including giving polygraphs to 10,000 employees, pending a high-level review.

20 February 2001

FBI agent Robert Philip Hanssen is arrested for espionage on behalf of the Soviet Union/Russia.

25 February 2001

US citizen and Hong Kong businessman Li Shaomin is arrested crossing the border into Shenzhen, China.

8 March 2001

Jean Wispleare pleads guilty to charge of attempted espionage.

9 March 2001

US military officials dismiss all charges against Daniel King—accused of passing secrets to Moscow in 1994—because a trial would have exposed more secrets.

16 March 2001

Former British GCHQ employee Geoffrey Prime is freed from prison after serving half his 38-year prison sentence for passing UK secrets to the KGB.

20 March 2001

Media reports that Chinese PLA Senior Colonel Xu Junping was missing since last December during a visit to the United States.

21 March 2001

United States orders 50 Russian diplomats expelled as suspected spies in response to the Robert Hanssen espionage case.

23 March 2001

Russia orders 50 US diplomats to leave the country in its first retaliatory move over the expulsion of 50 Russian diplomats from the United States in a Cold War-style spy row.

31 March 2001

US Navy EP-3 aircraft monitoring Chinese military maneuvers collides with Chinese fighter sent to intercept it and makes emergency landing on Hainan island.

4 April 2001

China formally arrests Chinese-born US academic Gao Zhan on charges of accepting money from a foreign intelligence agency and participating in espionage activities in China.

8 April 2001

China detains Wu Jianming, a US citizen of Chinese origin, for alleged espionage activities against China on behalf of Taiwan.

12 April 2001

China releases the 24 American crewmembers of the US Navy EP-3 plane, which landed at the Chinese military base on Hainan island.

4 May 2001

FBI arrests Chinese scientists Hai Lin and Kai Xu and Chinese-born naturalized US citizen Yong Qing Cheng for attempting to send Lucent Technologies intellectual property to a Chinese state-owned technology firm.

7 May 2001

The United States resumes spy flights off the coast of China.

9 May 2001

Justice Department charges Takashi Okamoto and Hiroaki Serizawa, two Japanese scientists, with stealing cells and genetic materials from Cleveland Clinic Foundation, a top research center in Cleveland, then passing them along to a research institute in Japan.

26 May 2001

China arrests Chinese-born American Wu Juanmin on spying charges.

8 June 2001

Five Cubans, arrested on 12 September 1998, are convicted in Miami of conspiring to spy on the United States for Fidel Castro's communist regime.

26 June 2001

US Army Officer George Trofimoff is convicted of espionage.

29 June 2001

Mario Faget, who was convicted of disclosing classified information to Cuba, is sentenced to five years in prison.

5 July 2001

President Bush nominates federal prosecutor Robert Mueller as new Director of the FBI.

6 July 2001

Robert Hanssen pleads guilty to spying for Russia, avoids death penalty, gets life in prison; family to keep his FBI pension and house.

11 July 2001

US District Court dismisses appeal by Robert Kim against his nine-year prison term for spying for South Korea.

14 July 2001

China convicts US citizen Li Shaomin of spying for Taiwan and orders him deported.

24 July 2001

China convicts US-based scholar Gao Zhan of spying for Taiwan and sentences her to 10 years in prison. China also convicts US permanent resident and businessman Qin Guangguang of spying for Taiwan.

26 July 2001

China expels Gao Zhan and Qin Guangguang in effort to soothe relations with the United States.

24 August 2001

FBI arrests Brian Regan, a retired Air Force sergeant who worked for a government contractor and assigned to the National Reconnaissance Office, for espionage.

30 August 2001

US Customs arrests David Tzu Wvi Yang and Eugene You Tsai Hsu for attempting to export military encryption technology to China in violation of the Arms Control Act.

4 September 2001

FBI arrests Cuban "La Red Avispa" spy ring members George and Marisol Gari and charges them with espionage.

Former Justice Department prosecutor Robert Mueller becomes the sixth Director of the FBI.

20 September 2001

George and Marisol Gari pleads guilty to spy charges.

21 September 2001

FBI arrests Ana B. Montes, a senior analyst with the Defense Intelligence Agency, and charges her with espionage on behalf of Cuban intelligence.

27 September 2001

District Court judge sentences ex-Army Colonel George Trofimoff to life in prison for espionage on behalf of the Soviets.

28 September 2001

China frees Wu Jianmin after he "confessed to his crimes" and places him on an airplane to the United States.