Joint Publication 3-54

Joint Doctrine for Operations Security

Revision First Draft

13 January 2003

PREFACE

1. Scope

This publication ~~describes the use of operations security (OPSEC) in the planning, preparation, and execution of joint operations~~ provides fundamental principles and doctrine for planning, preparation, and execution of operations security (OPSEC) in joint operations. Additionally, it provides ~~the~~ procedures how to~~for the~~ conduct ~~of~~ OPSEC ~~survey~~assessments.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It establishes~~sets forth~~ doctrine and ~~to~~ governs ~~the~~ joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the ~~joint force commander (~~JFC~~)~~ or the combatant commander from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached, supporting, or supported to forces of another Service or when significant forces of one Service.~~ support forces of another Service.~~

b. The guidance in this publication is authoritative; as such, this doctrine ~~(~~or ~~JTTP)~~joint tactics, techniques, and procedures will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

For the Chairman of the Joint Chiefs of Staff:

JOHN P. ABIZAID
Lieutenant General, USA
Director, Joint Staff

Intentionally Blank

TABLE OF CONTENTS

PAGE

TAB

TAB

GLOSSARY

FIGURE

CHAPTER I

GENERAL

> *"If I am able to determine the enemy's dispositions while at the same time I conceal my own, then I can concentrate and he must divide."*
>
> **Sun Tzu,**
> **The Art of War, 400-320 BC**

1. Policy

Policy for joint operations security (OPSEC) is established by the Chairman of the Joint Chiefs of Staff (CJCS) Instruction 3213.01A, *Joint Operations Security*. Reference should be made to that document for information concerning responsibilities relating to joint OPSEC and for requirements for establishing joint OPSEC programs.

2. Definition

OPSEC is a process of **identifying critical information** and subsequently **analyzing friendly actions** attendant to military operations and other activities to:

a. **Identify** those **actions** that can be observed by adversary intelligence systems.~~;~~

b. **Determine** what **indicators hostile intelligence systems might obtain** that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that **eliminate or reduce** to an acceptable level **the vulnerabilities of friendly actions** to adversary exploitation.

3. Characteristics of OPSEC

a. OPSEC's most important characteristic is that **it is a process**. OPSEC is not a collection of specific rules and instructions that can be applied to every operation. **It is a methodology that can be applied to any operation or activity** for the purpose of denying critical information to an adversary.

b. Unlike security programs that seek to protect classified information, OPSEC is concerned with **identifying**, **controlling**, and **protecting the generally unclassified evidence** that is associated with sensitive operations and activities. **OPSEC and security programs must be closely coordinated** to ensure that all aspects of sensitive operations are protected.

c. OPSEC acknowledges that **commanders must be prepared to assume some degree of risk** when choosing whether or not to execute OPSEC measures. OPSEC measures ~~will~~may, in most cases, entail the expenditure of resources. In choosing to execute particular OPSEC measures, commanders must decide that the **assumed gain in secrecy outweighs the costs in resources**. If commanders decide not to execute certain measures because the costs outweigh the gain, then they are assuming risks. The OPSEC process requires that decision makers to directly address how much risk they are willing to assume.

4. Responsibilities

Listed below are the responsibilities for key OPSEC individuals and commands or organizations.

a. Chairman of the Joint Chiefs of Staff

(1) Advises and coordinates with the Secretary of Defense concerning joint OPSEC support to the combatant commands.

(2) Provides joint OPSEC policy, doctrine, and joint tactics, techniques, and procedures.

(3) Provides procedures for joint OPSEC planning joint operation planning and execution system (JOPES).

(4) Ensures that appropriate OPSEC measures are implemented during CJCS exercises.

b. Director for Operations (J-3), Joint Staff

(1) Executes primary Joint Staff responsibility for OPSEC.

(2) Designates OPSEC staff positions for the Joint Staff.

(3) Maintains a joint OPSEC lessons-learned data base as a subset of the Joint Universal Lessons Learned System data base maintained by the Director for Operational Plans and Interoperability (J-7), Joint staff, to support OPSEC planning and training by the Joint Staff, Services, combatant commands, and Defense agencies.

(4) Establishes and maintains an OPSEC orientation program for Joint Staff officers, enlisted personnel, and civilians.

(5) Assists joint agencies and commands in arranging national interagency participation in OPSEC assessments.

(6) Coordinates with J-7, Joint Staff, to ensure that OPSEC is adequately addressed in operation plans (OPLANs) and contingency plans (CONPLANs) and is evaluated.

(7) Assigns an OPSEC liaison officer during periods of crisis and during CJCS exercises to assist all Joint Staff elements in integrating OPSEC into crisis management planning efforts. The OPSEC liaison officer will also serve as a point of contact to coordinate OPSEC issues with the combatant commands, Defense agencies, and Services.

(8) Establishes the OPSEC Executive Groups (OEG), as necessary, composed of members of the Joint Staff, Services, and appropriate agencies, to address specific OPSEC issues, such as problems relating to OPSEC programs that involve multiple commands or agencies.

(9) Coordinates with NSA, Interagency OPSEC Support Staff (IOSS) and Defense Threat Reduction Agency (DTRA) for OPSEC support.

c. **Services Chiefs**

(1) Provide Service OPSEC policy, doctrine, and planning procedures consistent with joint OPSEC policy, doctrine, and guidance.

(2) Provide joint OPSEC awareness training assistance for general populations, leadership, and OPSEC program managers.

(3) Designate a joint OPSEC program officer in the operations element of the Service headquarters.

(4) Designate representatives to Joint Staff OEGs, when required.

(5) Provide joint OPSEC lessons learned to the J-3 and J-7, Joint Staff, for

inclusion in the joint OPSEC lessons-learned database.

(6) Provide to J-3, Joint Staff, Deputy Director of Information Operations (DDIO, copies of all current Service OPSEC program directives and/or policy implementation documents.

(7) Organized teams to conduct vulnerability assessments of subordinate commands.

d. **Combatant Commanders**

(1) Provide OPSEC guidance for all command operations, exercises, and other joint activities of the command.

(2) Provide OPSEC guidance and identify command critical information to all supporting combatant commands, Services, other agencies, and appropriate public affairs offices.

(3) Coordinate OPSEC measures and their execution with other commands and agencies of those activities such as strategic C2 and counterdrug operations that cross command boundaries. Report any unresolved issues to J-3, Joint Staff, for assistance.

(4) Plan for and execute OPSEC measures in support of assigned missions

during peacetime, crisis, and war.

(5) Conduct OPSEC assessments in support of command operations.

(6) Designate an OPSEC program officer in the J-3 element of the command headquarters.

(7) Conduct annual OPSEC program reviews. Identify areas requiring additional CJCS guidance, assistance, or clarification to the J-3, Joint Staff, and DDIO.

(8) Provide OPSEC lessons learned to the J3 and J-7, Joint Staff, for inclusion in the joint OPSEC lessons-learned database.

(9) Provide to J-3, Joint Staff, DDIO copies of all current command OPSEC program directives and/or policy implementation documents.

(10) Provide joint OPSEC awareness training to assigned organizations.

e. **OPSEC Program Officer**

(1) Advise the commander on all OPSEC-related matters and for the daily management of the organization's OPSEC program.

(2) Recommend OPSEC guidance to the commander.

(3) Participate in IO planning.

(4) Develop, maintain, and execute the organization's OPSEC program to include writing the organization's policy and guidance documents.

(5) Coordinate and/or conduct OPSEC assessments, both command and formal.

(6) Coordinate appropriate intelligence and counterintelligence support.

(7) Develop and maintain organizational OPSEC lessons-learned database.

(8) Coordinate organizational OPSEC education and training.

(9) Coordinate with security program officers and public affairs officers.

f. **Director, Defense Intelligence Agency (DIA)**

(1) Establishes and maintains an OPSEC training program for DIA civilian and military personnel and attendees at the Defense Intelligence College.

(2) Designates an agency joint OPSEC program officer.

(3) Designates representatives to Joint Staff OEGs, as required.

(4) Identifies, reviews, and validates DIA and other department of defense (DOD) counterintelligence threat assessment documents for Joint Staff use.

(5) Conducts analysis of the foreign intelligence collection threat for required nations and organizations for use in OPSEC measures. Provides results to the Chairman of the Joint Chiefs of Staff, Chiefs of the Services, Combatant Commanders, and heads of Defense agencies.

g. **Director, National Security Agency (NSA), Interagency OPSEC Support Staff (IOSS)**

(1) Assists DOD components in establishing OPSEC programs, as requested.

(2) Provides interagency OPSEC training courses.

(3) Designates representative to Joint Staff OEGs, as required.

(4) Collaborates with the heads of the DOD components by providing:

(a) Technical OPSEC assessment support to DOD components to assist them in identifying their OPSEC vulnerabilities.

(b) When requested, recommendations relating to doctrine, methods, and procedures to minimize those vulnerabilities.

(c) Communications and computer security support for OPSEC assessments.

(d) Signal Intelligence (SIGINT) support for OPSEC threat development.

(e) Red and Blue team OPSEC assessments.

h. **Other Defense Agencies and Joint Activities**

(1) Designate an agency joint OPSEC Program Officer.

(2) Coordinate OPSEC programs and activities with commands and other agencies, as required.

(3) Provide representatives to OEGs, as required.

~~5Fundamentals of Command and Control Warfare (C2W)~~5. Activities Related to OPSEC

a. **Increasingly complex information systems** are being integrated into traditional warfighting disciplines such as mobility; logistics; and command, control, communications, computers, and intelligence (C4I). Many of these systems are designed and employed with **inherent vulnerabilities** that are, in many cases, the unavoidable consequences of enhanced functionality, interoperability, efficiency, and convenience to users. The low cost associated with such technology makes it **efficient and cost effective** to extend capabilities (and vulnerabilities) to an unprecedented number of users. The **broad access** to, and use of, these information systems enhance warfighting. However, **these useful capabilities induce dependence, and that dependence creates vulnerabilitie**s. These information systems are a **double-edged sword** — on one edge representing areas that warfighting components must protect, while on the other edge creating new opportunities that can be exploited against adversaries or used to promote common interests.

b. **OPSEC and Information Operations (IO). IO** are actions taken to affect adversary information and information systems while defending one's own information and information systems. OPSEC is one of the core competencies of IO. OPSEC supports, and is integrated with, the other elements of IO to deny adversary commander the information needed for effective decision making and to focus and prioritize IO countermeasures to protect only truly critical information (See Figure I-1).

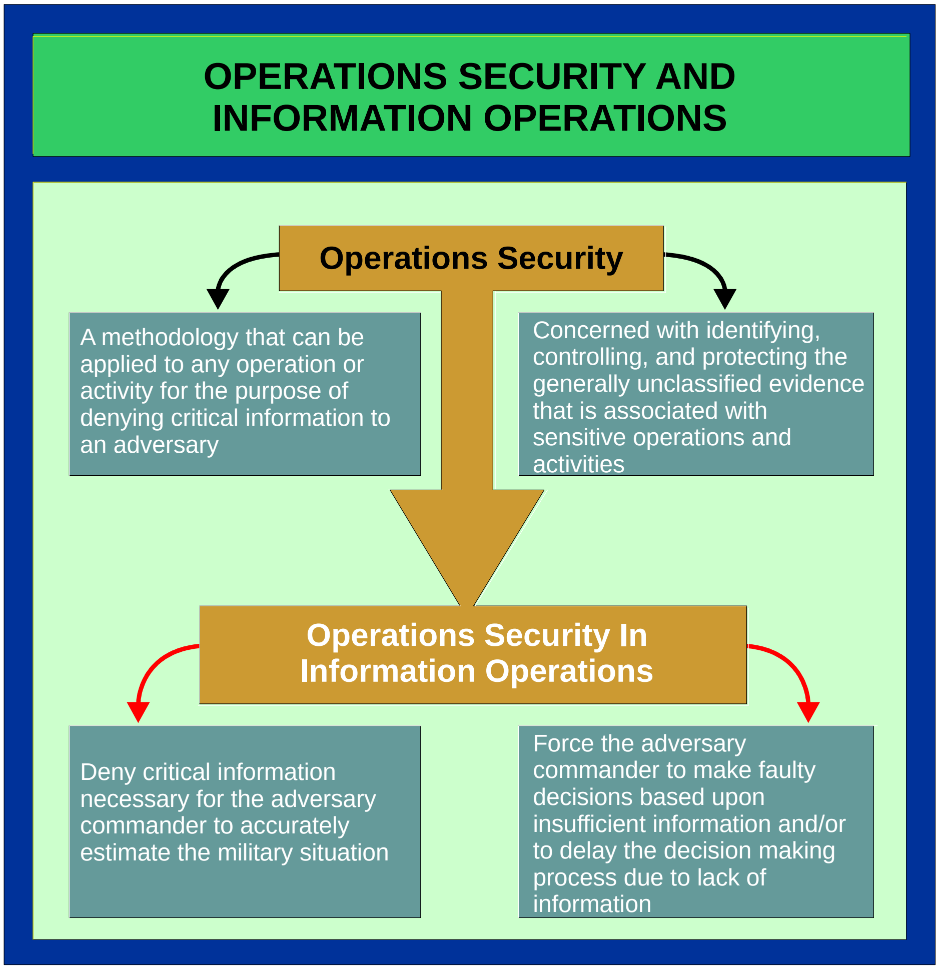

OPERATIONS SECURITY AND INFORMATION OPERATIONS
Operations Security
A methodology that can be applied to any operation or activity for the purpose of denying critical information to an adversary
Concerned with identifying, controlling, and protecting the generally unclassified evidence that is associated with sensitive operations and activities
Operations Security In Information Operations
Deny critical information necessary for the adversary commander to accurately estimate the military situation
Force the adversary commander to make faulty decisions based upon insufficient information and/or to delay the decision making process due to lack of information

Figure I-1. Operations Security and Information Operations ~~Command and Control Warfare~~

(1) **OPSEC contributes to offensive and defensive IO** by slowing the adversary's decision cycle and providing opportunity for easier and quicker attainment of friendly objectives. OPSEC focuses on having a good understanding of the adversary decision maker's ability to collect reliable, adequate, timely intelligence, and, when integrated with other capabilities, shapes to our advantage the adversary's knowledge and beliefs about our operations. OPSEC denies the adversary critical information about friendly capabilities and intentions needed from effective and timely decision making,

leaving the adversary vulnerable to other offensive capabilities. Early integration of OPSEC into mission planning is essential to reduce a friendly operation's revealing indicators to a minimum and better target the adversary's decision making process.

(2) Many different **capabilities and activities must be integrated** to achieve a coherent IO strategy. Capabilities and activities such as, psychological operations (PSYOP), military deception, OPSEC, electronic warfare (EW), and physical destruction, can be employed to achieve broader IO objectives that are outside the C2 target set. **Intelligence and communications support** are critical to conducting offensive and defensive IO. The **thoughtful design and correct operation** of information systems are fundamental to the successful conduct of IO. Moreover, to be successful, **IO must be integrated with other operations** (air, land, sea, space, and special) and contribute to national and military objectives.

See Joint Pub 3-13, Joint Doctrine for Information Operation.

(3) **Offensive IO involve the integrated use of assigned and supporting capabilities and activities**, mutually supported by intelligence, **to affect adversary decision makers and achieved or promote specific objectives.**

(a) These assigned and supporting capabilities and activities include, but are not limited to, OPSEC, military deception, PSYOP, EW physical attack/destruction, and special information operations (SIO), and may include computer network attack. (CNA).

(b) Offensive IO may be conducted in a variety of situations and circumstances across the range of military operations and may have their **greatest impact in peace and initial stages of a crisis.** Beyond the threshold of crisis, offensive IO can be **a critical force enabler** for the joint forces commander (JFC). Offensive IO may be conducted **all levels of war**---strategic, operational, and tactical ---throughout the battlespace.

(4) **Defensive IO integrate and coordinated policies and procedures, operations, personnel, and technology to protect and defend information and information systems**. Defensive IO are conducted through information assurance, OPSEC, physical security, counterdeception, counterpropaganda, counterintelligence, EW, and SIO.

(a) Defensive IO ensure the **necessary protection and defense of information and information systems** upon which joint forces depend to conduct operations and achieve objectives.

(b) **Four interrelated processes support defensive IO:** information environment protection, attack detection, capability restoration, and attack response. Because they are so interrelated, full integration of the offensive and defensive components of IO is essential.

c. **OPSEC and Information Warfare** are IO conducted in time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Applying the OPSEC process and OPSEC countermeasures throughout the planning of operations in crisis or conflict will ensure the essential secrecy necessary for success.

~~c.~~ ~~C2W is the integrated use of psychological operations (PSYOP), military deception, OPSEC, electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control (C2) capabilities while protecting friendly C2 capabilities against such actions. C2W is a warfighting application of information warfare (IW) in military operations and is a subset of IW.~~

~~(MOOTW). C2W is planned and executed by combatant commanders, subunified commanders, and joint task force commanders. C2W efforts are focused within a commander of a combatant command's area of responsibility or a commander, joint task force's joint operations area and their area of interest (AOI).~~ ~~**C2W is an essential part of any joint military operation**~~ ~~opposed or threatened by an organized military paramilitary force, or terrorist organizations. It is an integral part of an overall campaign plan. C2W applies to all phases of an operation, including those before, during and after actual hostilities.~~

~~c.~~ ~~**The elements of C2W**~~ ~~(PSYOP, military deception, OPSEC, EW, physical destruction)~~ ~~**can support land, sea, air, and space operations**~~. ~~Although C2W as defined is composed of these five elements, in practice other warfighting capabilities may~~

~~be employed as part of C2W to attack or protect a C2 "target set." The level of applicability of the various C2W elements is dependent on the assigned mission and the circumstances, targets, and resources available.~~ ~~**C2W provides a framework that promotes synergy between the individual elements**~~ ~~to produce a significant warfighting advantage. Even in MOOTW, C2W offers the military commander lethal and nonlethal means to achieve the assigned mission while deterring war and/or promoting peace.~~

~~d. Effective C2W provides to the joint force commander (JFC) an ability to~~ ~~**shape the adversary commander's estimate of the situation**~~ ~~in the theater of operations. It may even be possible to convince an adversary that the United States has "won" prior to engaging in battle, resulting in deterrence and preempting hostilities.~~

~~e.~~ ~~**A successful C2W**~~ ~~effort will contribute to the security of friendly forces, bring the adversary to battle (if appropriate) at a disadvantage, help seize and maintain the initiative, enhance freedom of maneuver, contribute to surprise, isolate adversary forces from their leadership, and create opportunities for a systematic exploitation of adversary vulnerabilities.~~

~~f~~___~~.~~ ~~**Effective C2W**~~ ~~operations~~ ~~**influence, disrupt, or delay the adversary's decision cycle.**~~ ~~This decision cycle is supported by a C2 system which does not merely consist of a commander and the infrastructure to communicate orders. It encompasses all the capabilities, thought processes, and actions that allow a commander to correctly observe~~

~~the AOI; assess what those observations imply about the operation; use assessments to make timely, effective decisions; and communicate those decisions as orders to subordinate commanders to control the course of an operation. The execution of orders on both sides of an operation alters the situation in the operational area. These changes, in turn, must be **observed, assessed, and acted upon in a continuous process**. This process can be thought of as a "decision cycle."~~

~~g. **Synchronized C2W** operations **should enable a JFC to operate "inside" an adversary's decision cycle** by allowing the JFC to process information through the C2 decision cycle faster than an adversary commander. Initiative is fundamental to success in military operations. In C2W, both C2-attack and C2-protect operations contribute to gaining and maintaining military initiative.~~

Since the news media potentially can be a lucrative source of information to adversaries, OPSEC planners must work closely with public affairs personnel to avoid inadvertent disclosure of critical information.

~~**6. OPSEC and Command and Control Warfare**~~

~~See Figure I-1.~~

~~a. **OPSEC is concerned with denying critical information about friendly forces to the adversary.** In C2W, the threat to OPSEC is ultimately the adversary commander. Denial of critical information about friendly capabilities and limitations may result in flawed command decisions that prove devastating to the adversary force. The emphasis of OPSEC as a part of an overall C2W effort should be **to deny critical information necessary for the adversary commander to accurately estimate the military situation**. The intent of OPSEC in C2W should be to force the adversary commander to make faulty decisions based upon insufficient information and/or to delay the decision making process due to a lack of information.~~

~~b.~~

MEDIA IN DESERT SHIELD AND DESERT STORM

As in all previous American conflicts, the rules for news coverage of Operations DESERT SHIELD and DESERT STORM were driven by the need to balance the requirements of operational security against the public's right to know about ongoing military operations. DOD policy calls for making available "timely and accurate information so the public, Congress, and the news media may assess and understand the facts about national security and defense strategy," withholding information "only when disclosure would adversely affect national security or threaten the safety or privacy of the men and women of the Armed Forces." The news media feel compelled to report as much information about current newsworthy events as possible.

The challenge to provide full news coverage of Operations DESERT SHIELD and DESERT STORM was complicated by several factors:

• The host nation, closed to western media before the operation began, was reluctant to permit reporters to enter the country and was concerned about reporting of cultural sensitivities.

• More than 1,600 news media representatives eventually massed in Saudi Arabia to report about the war.

• The combat actions of Operation DESERT STORM used high technology, involved

long-range weapons, and occurred on and over a distant, vast, open desert and from ships operating in adjacent bodies of water.

• The combined armor and airmobile attacks and drives through Kuwait and Iraq were rapid.

• This was the first major American war to be covered by news media able to broadcast reports instantaneously to the world, including the enemy.

From the beginning of the crisis, the Department of Defense worked closely with Central Command (CENTCOM), the Joint Staff (JS), the Services, and news media organizations to balance the media's needs with the military's ability to support them and its responsibility to preserve US combat forces' operational security. The goal was to provide as much information as possible to the American people without endangering the lives or missions of US military personnel.

SOURCE: DOD Final Report to Congress
Conduct of the Persian Gulf War, April 1992

d. **OPSEC and the News Media.** **The inevitable presence of the news media during military operations complicates OPSEC.** As part of the global information infrastructure, the news media portrays and offers commentary on military activities on the battlefield—both preparatory to and during battle. News media portrayal of military activities prior to hostilities can **help to deter actual hostilities** and/or **build public support for inevitable hostilities**. By portraying the presence of US and/or multinational military forces in or en route to the operational area, **news media stories can demonstrate the readiness, commitment and resolve of the United States and its multinational partners** to commit military forces to battle if necessary to protect US and/or multinational interests, lives, or property. However, the presence of the news media in the operational area, with the capability to transmit information on a real-time basis to a worldwide audience, has the potential to be a **lucrative source of information to adversaries**. OPSEC planners must keep these considerations in mind when determining which aspects of a military operation are "critical information" that must be denied to the adversary and shared with the media. OPSEC planners must work closely with military public affairs personnel to develop guidelines that can be used by both military and news media personnel to **avoid inadvertent disclosure of critical information** that could, ultimately, increase the risk to the lives of US and/or multinational military personnel.

e. **OPSEC and Public Affairs (PA).** PA seeks a timely flow of information to both external and internal audiences. Coordination of PA and OPSEC planners is required to ensure that PA initiatives support the commander's overall objectives, consistent with DOD principles of information. PA and OPSEC efforts will be integrated consistent with policy or statutory limitation and security. PA activities will not be used as a military deception capability or provide disinformation to internal or external audiences.

See JP 3-61, Doctrine for Public Affairs in Joint Operations.

f. **OPSEC and Civil Affairs (CA).** CA activities are an important contributor to OPSEC because of their ability to interface with key organizations and individuals in the information environment. CA activities can support and assist the achievement of OPSEC by coordinating with, influencing, developing, or controlling indigenous infrastructures in foreign operational areas. These activities may occur before, during, subsequent to, or in the absence of other military actions.

See JP 3-57, Doctrine for Joint Civil Affairs.

g. OPSEC and Intelligence Support

(1) Intelligence support is critical to the planning, execution, and assessment of OPSEC. The joint staff intelligence (J-2) representative(s) should be the liaison for intelligence support for all OPSEC planning.

(2) Intelligence must be timely, accurate, usable, complete, relevant, objective, and detailed to support OPSEC.

(3) Intelligence efforts must be focused to support OPSEC across the range of military operations at all levels of war. Due to the widespread dependence and capability in information technologies, US military forces now depend more on individual operators at all levels to collect, conduct initial analysis, disseminate, and act on information. Thus everyone, not just intelligence specialists, must be part of the threat assessment.

~~c.~~ ~~**Denial of critical information to the**~~ ~~adversary~~ ~~**commander**~~ ~~contributes to uncertainty and slows the adversary's decision cycle. Critical information can be hidden by such traditional OPSEC measures as action control, countermeasures, and counteranalysis.~~ ~~**Counterintelligence support is an integral part of successful OPSEC.**~~ ~~PSYOP and military deception personnel also work closely with OPSEC planners to mutually support their respective efforts.~~

~~d. Critical information denied to an adversary can be replaced or refocused to support the commander's goals through military deception and/or PSYOP, if use of those~~

~~elements has been approved at the appropriate level. In C2W,~~ ~~**operational planners concerned with OPSEC should also coordinate with C2 planners, EW planners, and targeteers**~~ ~~to deny critical information to the adversary commander. The OPSEC process may also identify for attack particular adversary collection, processing, analysis, and distribution systems in order to deny the adversary commander critical information by forestalling that commander's ability to collect it.~~

CHAPTER II~~I~~

THE OPSEC PROCESS

> *"He passes through life most securely who has least reason to reproach himself with complaisance toward his enemies."*
>
> **Thucydides,**
> **History of the Peloponnesian Wars, 404 BC**

1. General

a. **OPSEC planning is accomplished through the use of the OPSEC process.** This process, when used in conjunction with the joint planning processes, provides the information required to write the OPSEC section of any plan or order. OPSEC planning is done in close coordination with the overall ~~C2W~~IO planning effort. ~~and with the planning of the other C2W components.~~

b. The OPSEC process is applicable to all military operations and other activities. Use of the process ensures that the resulting OPSEC measures address all significant aspects of the particular situation and are balanced against operational requirements. OPSEC is a continuous and iterative process. **The OPSEC process consists of five distinct actions.** These OPSEC actions are applied~~ in a **sequential or adaptive manner**~~ continuously during ~~OPSEC~~ joint operations planning. In dynamic situations, however, individual actions may be ~~revisited~~re-evaluated at any time. New information about the adversary's intelligence collection capabilities, for instance, would require a new analysis of threats.

c. An understanding of the following terms is required before the process can be explained.

(1) **Critical Information.** Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

(2) **OPSEC Indicators.** Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

(3) **OPSEC Vulnerability.** A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making.

2. The OPSEC Process

a. The OPSEC process consists of five actions (Figure II-1). OPSEC, also, has an adaptive operation security process (Figure II-2).

b. ~~OPSEC Action 1 —~~Identification of Critical Information

- ~~While assessing and comparing friendly versus adversary capabilities during the planning process for a specific operation or activity, **the commander and staff seek to identify the questions that they believe the adversary will ask** about friendly intentions, capabilities, and activities. **These questions are the essential elements of friendly information (EEFI).** In an operation plan or order, the EEFI are listed in Appendix 3 (Counterintelligence) to Annex B (Intelligence).~~

(1) **Critical information is ~~a subset of EEFI.~~** ~~It is only that~~ information that is vitally needed by an adversary. The identification of critical information is important in that **it focuses the remainder of the OPSEC process on protecting vital information** rather than attempting to protect all classified or sensitive information.

(2) **Critical information is listed in the OPSEC portion of an operation plan or order.** Generic critical information lists can be developed before hand to assist in identifying the specific critical information. Some general categories of critical information are provided in Appendix A, "Examples of OPSEC Critical Information."

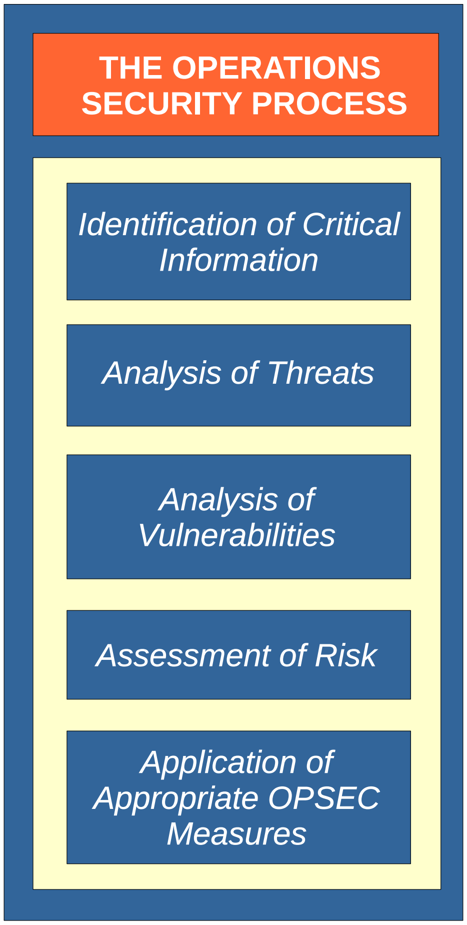

THE OPERATIONS SECURITY PROCESS
Identification of Critical Information
Analysis of Threats
Analysis of Vulnerabilities
Assessment of Risk
Application of Appropriate OPSEC Measures

Figure II-1. The Operations Security Process

c. ~~OPSEC Action 2 —~~Analysis of Threats

(1) This action involves the research and analysis of **intelligence information**, **counterintelligence**, **reports**, and **open source information** to identify who the likely adversaries are to the planned operation. PSYOP provide information on adversarial personalities that assist in developing a threat analysis.

(2) **The operations planners**, working with the intelligence and counterintelligence staffs and assisted by the OPSEC program ~~personnel~~officer, **seek**

answers to the following critical information questions:

(a) Who is the adversary? (Who has the intent and capability to take action against the planned operation?)

(b) What are the adversary's goals? (What does the adversary want to accomplish?)

(c) What is the adversary's strategy for opposing the planned operation? (What actions might the adversary take?)

(d) What critical information does the adversary already know about the operation? (What information is it too late to protect?)

(e) What are the adversary's intelligence collection capabilities?

(3) Detailed information about the adversary's intelligence collection capabilities can be obtained from the command's counterintelligence and intelligence organizations. ~~In addition to knowing about the adversary's capabilities,~~ ~~**it is important to understand how the intelligence system processes the information that it gathers**~~~~.~~ ~~Appendix B, "The Intelligence Threat," discusses the general characteristics of intelligence systems.~~

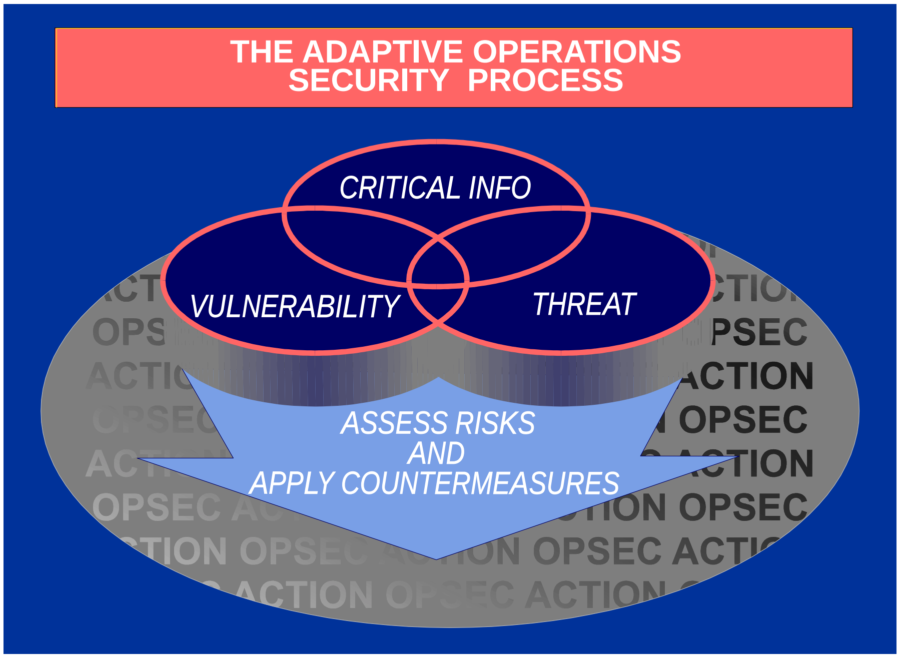


Figure II-2. The Adaptive Operations Security Process

d. ~~OPSEC Action 3 —~~Analysis of Vulnerabilities

(1) The purpose of this action is to **identify an operation's or activity's OPSEC vulnerabilities**. It requires examining each aspect of the planned operation to identify any OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. A vulnerability exists when the adversary is capable of collecting an OPSEC indicator, correctly analyzing it, and then taking timely action. The adversary can then exploit that vulnerability to obtain an advantage.

> *"Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing."*
>
> **Frederick the Great**
> **The Art of Modern War, 1940**

(2) Continuing to work with the intelligence and counterintelligence staffs, the operations planners seek answers to the following critical information questions:

(a) What indicators (friendly actions and open source information) of critical information not known to the adversary will be created by the friendly activities that will result from the planned operation?

(b) What indicators can the adversary actually collect?

(c) What indicators will the adversary be able to use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?)

(3) See Appendix ~~C~~B, "OPSEC Indicators," for a detailed discussion of OPSEC indicators.

~~When conducting joint operations, a~~All personnel must understand the adversary's intelligence ~~collection~~ capabilities to collect information ~~-~~and take ~~action to~~OPSEC measures to deny the use of those capabilities.

e. ~~OPSEC Action 4 —~~Assessment of Risk

(1) This action has two components. First, **planners analyze the OPSEC vulnerabilities** identified in the previous action and **identify possible OPSEC measures** for each vulnerability. Second, **specific OPSEC measures are selected for execution** based upon a risk assessment done by the commander and staff.

(2) OPSEC measures reduce the probability of the adversary either collecting the indicators or being able to correctly analyze their meaning.

(a) **OPSEC measures can be used to:** (1) Prevent the adversary from detecting an indicator; (2) Provide an alternative analysis of an indicator; and/or (3) Attack the adversary's collection system.

(b) OPSEC measures include, among other actions, cover, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against the adversary's intelligence system.

(c) **More than one possible measure may be identified for each vulnerability.** Conversely, a single measure may be used for more than one vulnerability. The most desirable OPSEC measures are those that combine the highest possible protection with the least effect on operational effectiveness. Appendix C~~D~~, "Operations Security Measures," provides examples of OPSEC measures.

(3) **Risk assessment** requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

(a) **OPSEC measures usually entail some cost** in time, resources, personnel, or interference with normal operations. If the cost to mission effectiveness exceeds the harm that an adversary could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires command involvement.

(b) Typical questions that might be asked when making this analysis include the following:

1 What risk to effectiveness is likely to occur if a particular OPSEC measure is implemented?

2 What risk to mission success is likely to occur if an OPSEC measure is not implemented?

3 What risk to mission success is likely if an OPSEC measure fails to be effective?

(c) **The interaction of OPSEC measures must be analyzed.** In some situations, certain OPSEC measures may actually create indicators of critical information. For example, ~~the~~ camouflaging ~~of~~ previously unprotected facilities ~~could be an~~ can indicat~~or~~e ~~of~~ preparations for military action.

(4) **The selection of measures** must **be coordinated with ~~the~~ other components of ~~C2W~~IO.** Actions such as jamming of intelligence nets or the physical destruction of critical intelligence centers can be used as OPSEC measures. Conversely, military deception and PSYOP plans may require that OPSEC measures not be applied to certain indicators in order to project a specific message to the adversary.

f. ~~OPSEC Action 5 —~~ Application of Appropriate OPSEC Measures

(1) ~~In this step, t~~The command **implements the OPSEC measures** selected in ~~Step 4~~ the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans. Before countermeasures can be selected, security objectives and critical information must be known, indicators identified, and vulnerabilities assessed.

(2) A general countermeasure strategy should be to:

(a) Minimize predictability from previous operations.

(b) Determine detection indicators and protect them by elimination, control or deception.

(c) Conceal indicators of key capabilities and potential objectives.

(3) During the execution of OPSEC measures, **the reaction of adversaries to the measures is monitored to determine their effectiveness and to provide feedback**. Planners can use ~~that~~ feedback to adjust ongoing activities and for future OPSEC planning. Provisions for feedback must be coordinated with the command's intelligence and counterintelligence staffs to ensure ~~that the~~ requirements to support OPSEC receive the appropriate priority. In addition to intelligence and cryptologic sources providing feedback, OPSEC assessments can provide useful information relating to the success of OPSEC measures.

A key action during the OPSEC process is to analyze potential vulnerabilities to joint forces. It requires identifying any OPSEC indicators that could reveal critical information about the operation, such as, increased troop movement.

3. OPSEC Assessment

An OPSEC assessment is an **intensive application of the OPSEC process** to an existing operation or activity by a multi-disciplined team of experts. Assessments are essential for **identifying requirements** for additional measures and for **making necessary changes** in existing measures. An OPSEC assessment is a good tool to validate OPSEC programs and organizational practices to protect critical information in operations. NSA, IOSS and Services have or can coordinate Red and Blue Teams designed to act as an adversary to verify OPSEC plans and procedures. Appendix D, "Procedures for OPSEC Assessments," describes the procedures for conducting OPSEC assessments.

CHAPTER III

OPSEC PLANNING

> *"To keep your actions and your plans secret always has been a very good thing . . . Marcus Crassus said to one who asked him when he was going to move the army: 'Do you believe that you will be the only one not to hear the trumpet?"*
>
> **Niccolo Machiavelli,**
> **The Art of War, 1521**

1. General

a. Despite extraordinary changes in the world geopolitical environment in recent years, many nations and organizations are actively engaged in conducting intelligence operations against the United States and its Armed Forces. Open-source material (including the media and the Internet) and observations of US activities and operations are major sources of information for the adversary. This is especially true of terrorist organizations.

b. In order to prevent adversaries (or potential adversaries) from gaining valuable intelligence about friendly operations, joint forces must plan and execute OPSEC measures. To be effective, OPSEC measures must be considered as early as possible during mission planning and ~~then be~~ appropriately revised to keep pace with any changes in current operations and adversarial threats (conventional and asymmetric).

c. Joint OPSEC planning and execution occur as part of the command's or organization's ~~C2W~~IO effort. The commander's objectives for ~~C2W~~IO are the basis for

OPSEC planning. In addition to directly supporting the accomplishment of the commander's objectives, the use of OPSEC measures in support of the other components of ~~C2W~~IO must also be considered during OPSEC planning.

2. OPSEC ~~Planning~~ Factors

____The following factors must be considered when conducting OPSEC planning:

____a. The commander plays the critical role. OPSEC planning guidance must be provided as part of the commander's ~~C2W~~IO planning guidance to ensure that OPSEC is considered during the development of friendly courses of action (COAs). The commander must ensure that all personnel are aware of the appropriate OPSEC measures. OPSEC is everyone's responsibility.

While planning joint operations, including those requiring highly visible deployments, OPSEC measures must be considered as early as possible to prevent adversaries from gaining valuable intelligence.

____b. OPSEC is an operational function, not a security function. OPSEC planning ~~must~~

~~be done ~~is performed by the J-3 operations planners. The J-3 planners are assisted by the organization's OPSEC program ~~personnel~~officer and appropriate planners from other staff elements. Intelligence support is particularly important in determining the threat to friendly operations~~ and in~~, assessing friendly vulnerabilities, determining the adversary's capabilities, and predicting the adversary's COAs.

c. JFCs should establish a fully functional IO cell. The JFC's staff, which includes the IO cell, develops and promulgates guidance and plans for IO that are passed to the components and supporting organizations and agencies for decentralized planning and execution. The OPSEC program officer plays a vital role in the IO cell. The OPSEC officer coordinates combatant command or subordinate joint force command OPSEC activities and coordinates with the J-6 and J-3 planners for NSA's joint communications security (COMSEC) monitoring activity (JCMA) liaison.

d. Planning must focus on identifying and protecting critical information. Denying all information about a friendly operation or activity is seldom cost effective or realistic.

e. The ultimate goal of OPSEC is increased mission effectiveness. By preventing an adversary from determining friendly intentions or capabilities, OPSEC reduces losses to friendly units and increases the likelihood of achieving mission success.

f. OPSEC ~~should be~~ is one of the factors considered during the development and selection of friendly COAs. COAs will differ in terms of how many OPSEC indicators will be created and how easily those indicators can be managed by OPSEC measures. Depending upon how important maintaining secrecy is to mission success, OPSEC considerations may be a factor in selecting a COA.

g. OPSEC planning is a continuous process. During ~~the execution~~all phases of an operation, feedback on the success or failure of OPSEC measures is evaluated and the OPSEC plan is modified accordingly. Friendly intelligence and counterintelligence organizations, ~~communications security (~~COMSEC~~)~~ monitoring, and OPSEC ~~survey~~assessments are the primary sources for feedback information.

h. The ~~P~~public affairs officer (PAO) ~~should~~ participates in OPSEC planning to provide ~~their~~ assessments on the possible effects of media coverage and for the coordination of OPSEC measures to minimize those effects. The PAO ensures that the media pool, media clearances, media releases and authorization of video transmissions are within the established OPSEC measures.

See JP 3-61, Doctrine for Public Affairs in Joint Operations, *for further detail.*

i. OPSEC considers the integration, coordination, deconfliction and synchronization of PSYOP, that includes multinational information activities within the JFC's area of responsibility.

> *"O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence hold the enemy's fate in our hands."*
>
> **Sun Tzu, c. 500 BC**
> **The Art of War**

j. The termination of OPSEC measures must be addressed in the OPSEC plan to prevent future adversaries from developing countermeasures to successful OPSEC measures. ~~In some situations, it may be necessary for the~~ The OPSEC plan must ~~to~~ provide guidance on how to prevent the target of the ~~OPSEC~~post-execution operations as well as any interested third parties from discovering sensitive information relating to OPSEC during the post-execution phase.

3. OPSEC Planning Coordination

a. General. OPSEC coordination is continuous across **all phases of an operation** and **range of military operations** and **at every level of war.** OPSEC planning is integrated with post-conflict activities, which are transitioned, to a foreign military or government, United States nongovernmental organizations (NGOs), or peacekeeping forces.

b. **Joint Planning Group.** JFC's **normally establish a joint planning group (JPG)**, particularly at the JTF level. Early and continuous exchange of information and close coordination of planning activities between the JPG and the OPSEC representative is essential to successful integration of OPSEC planning in the overall Joint Operation Planning and Execution System (JOPES).

4. OPSEC Planning and Joint Operation Planning Processes

a. **Joint OPSEC Planning**. OPSEC planning in support of joint operations is accomplished through the application of the OPSEC process. The five actions that compose the OPSEC process are described in detail in Chapter II~~I~~, “The OPSEC Process.” Joint OPSEC planning is always done in conjunction with normal joint operation planning and is a part of the overall ~~C2W~~IO planning effort.

b. ~~**The**~~ **Campaign Planning Process.** A campaign is a series of related major operations that arrange tactical, operational, and strategic actions to accomplish strategic and operational objectives. They are joint in nature and serve as the focus for the conduct of war and military operations other than war. Although not formally part of the JOPES, campaign planning encompasses both deliberate and crisis action planning process. ~~There are three major planning processes for joint planning. Plans are proposed under different processes depending on the focus of a specific plan. The processes are labeled either campaign, deliberate, or crisis action planning, and are interrelated. They are described in Joint Pub 5-0, “Doctrine for Planning Joint Operations.”~~

(1) Combatant commanders translate national and theater ~~strategy~~ goals and objectives into strategic and operational concepts through the development of theater campaign plans. The campaign plan embodies the combatant commander’s strategic vision of the arrangement of related operations necessary to attain theater strategic objectives. Campaign planning encompasses both the deliberate and crisis action

planning processes. If the scope of contemplated operations requires it, campaign planning begins with or during deliberate planning. It continues through crisis action planning, thus unifying both planning processes. As stated in Joint Pub 1, ~~“~~*Joint Warfare of the Armed Forces of the United States,*~~”~~ “Campaign planning is done in crisis or conflict (once the actual threat, national guidance, and available resources become evident), but the basis and framework for successful campaigns is laid by peacetime analysis, planning, and exercises.” The degree to which the amount of work accomplished in deliberate planning may serve as the core for a campaign plan is directly dependent on the particular theater and objectives.

(2) Preparation of a campaign plan is appropriate when contemplated military operations exceed the scope of a single major operation. Campaign planning is appropriate to both deliberate and crisis action planning. During peacetime deliberate planning, combatant commanders prepare joint operation plans (OPLANs), including campaign plans, in direct response to taskings in the Joint Strategic Capabilities Plan. ~~Tasking for strategic requirements or major contingencies may require the preparation of several alternative plans for the same requirement using different sets of forces and resources to preserve flexibility. For these reasons, campaign plans are based on reasonable assumptions and are not normally completed until after the National Command Authorities (NCA) selects the course of action during crisis action planning. Deliberate plans may include elements of campaign planning; however, these elements will have to be updated as in any deliberate plan used at execution. Execution planning is conducted for the actual commitment of forces when conflict is imminent. It is based on~~

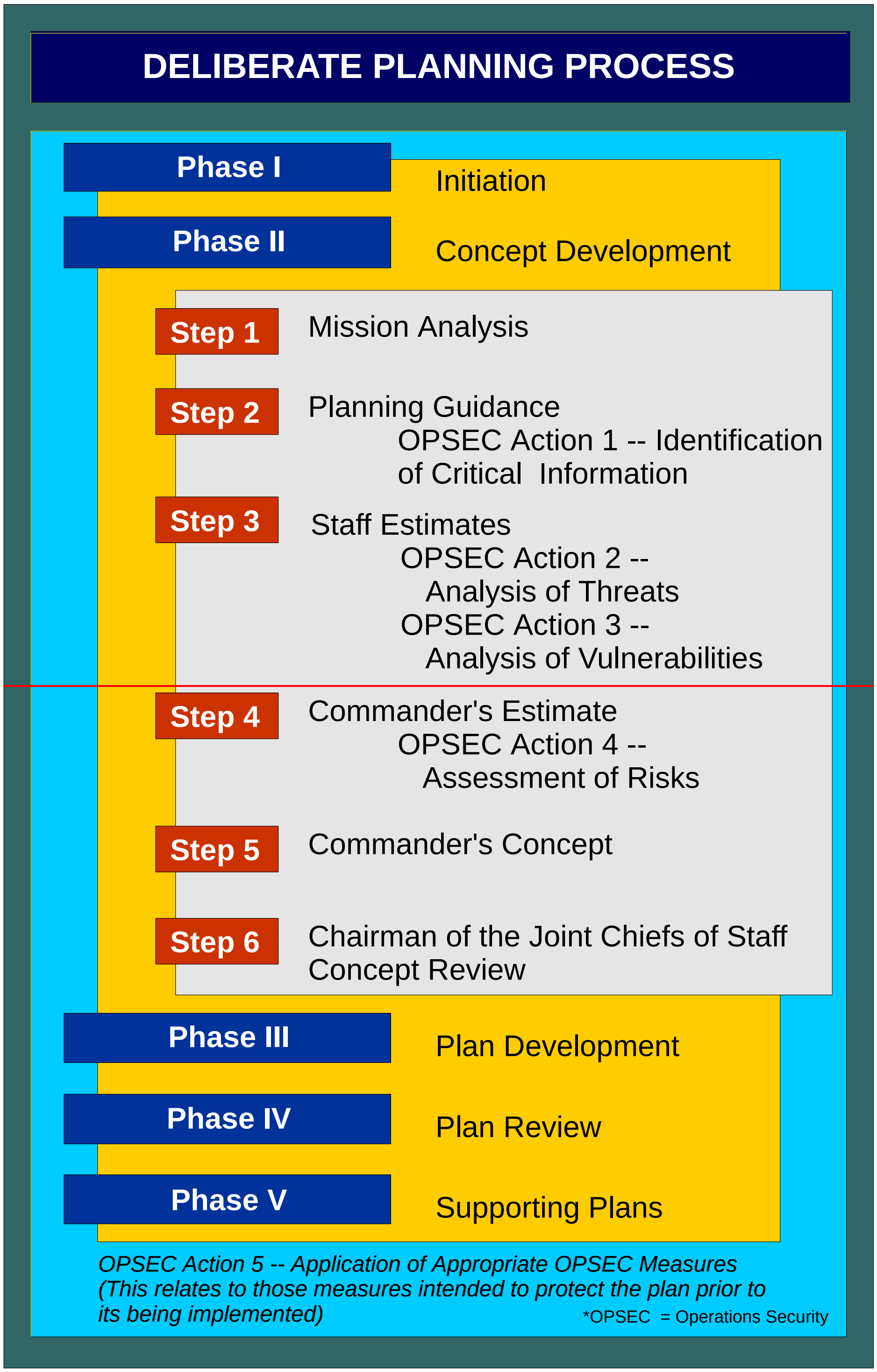
~~the current situation and includes deployment and initial employment of forces. When a crisis situation develops, an assessment is conducted that may result in the issuance of a CJCS WARNING ORDER. COAs are developed based on an existing OPLAN or operation plan in concept format (CONPLAN), if applicable. The combatant commander proposes COAs and makes any recommendations when the Commander's Estimate is forwarded to the NCA. The NCA selects a COA and, when directed, the Chairman issues a CJCS ALERT ORDER. The combatant commander now has the essential elements necessary for finalizing the construction of a campaign plan using the approved COA as the centerpiece of the plan. OPSEC planning is done the same as in crisis action planning (see Figure II-2).~~

See JP 5-0, Doctrine for Planning Joint Operations, *for further detail.*

c. **OPSEC and the Deliberate Planning Process.** ~~OPSEC planning relates to the Joint Operation Planning and Execution System (JOPES) deliberate planning process as shown in Figure II-1.~~When OPSEC planning is being conducted below the combatant command level, clear, two-way communications must be established to ensure the OPSEC chain of command is fully appraised of all OPSEC deliberate planning activities that may require synchronization, coordination, or deconfliction.

d. **OPSEC and the Crisis Action Planning Process.** ~~OPSEC planning relates to the JOPES crisis action planning process as shown in Figure II-2.~~ In contrast to deliberate planning, crisis action planning normally takes place in a compressed time period. In crisis action planning, coordination of the OPSEC plan is even more crucial than in deliberate planning. OPSEC planning is an integral part of the JOPES crisis action planning at the combatant command level. Additionally, OPSEC measures must continue during the post-execution phase of joint operations. Friendly forces have a tendency to become complacent during this timeframe. The adversary does not cease to monitor friendly activities for vulnerabilities and weakness.

~~f. OPSEC Plans Format. OPSEC plans are prepared as part of all joint operation plans and orders~~. ~~The format is found in Joint Pub 5-03.2, "Joint Operation Planning and Execution System, Vol II: (Planning and Execution Formats and Guidance)."~~



DELIBERATE PLANNING PROCESS

Phase I — Initiation

Phase II — Concept Development

Step 1 — Mission Analysis

Step 2 — Planning Guidance
OPSEC Action 1 -- Identification of Critical Information

Step 3 — Staff Estimates
OPSEC Action 2 -- Analysis of Threats
OPSEC Action 3 -- Analysis of Vulnerabilities

Step 4 — Commander's Estimate
OPSEC Action 4 -- Assessment of Risks

Step 5 — Commander's Concept

Step 6 — Chairman of the Joint Chiefs of Staff Concept Review

Phase III — Plan Development

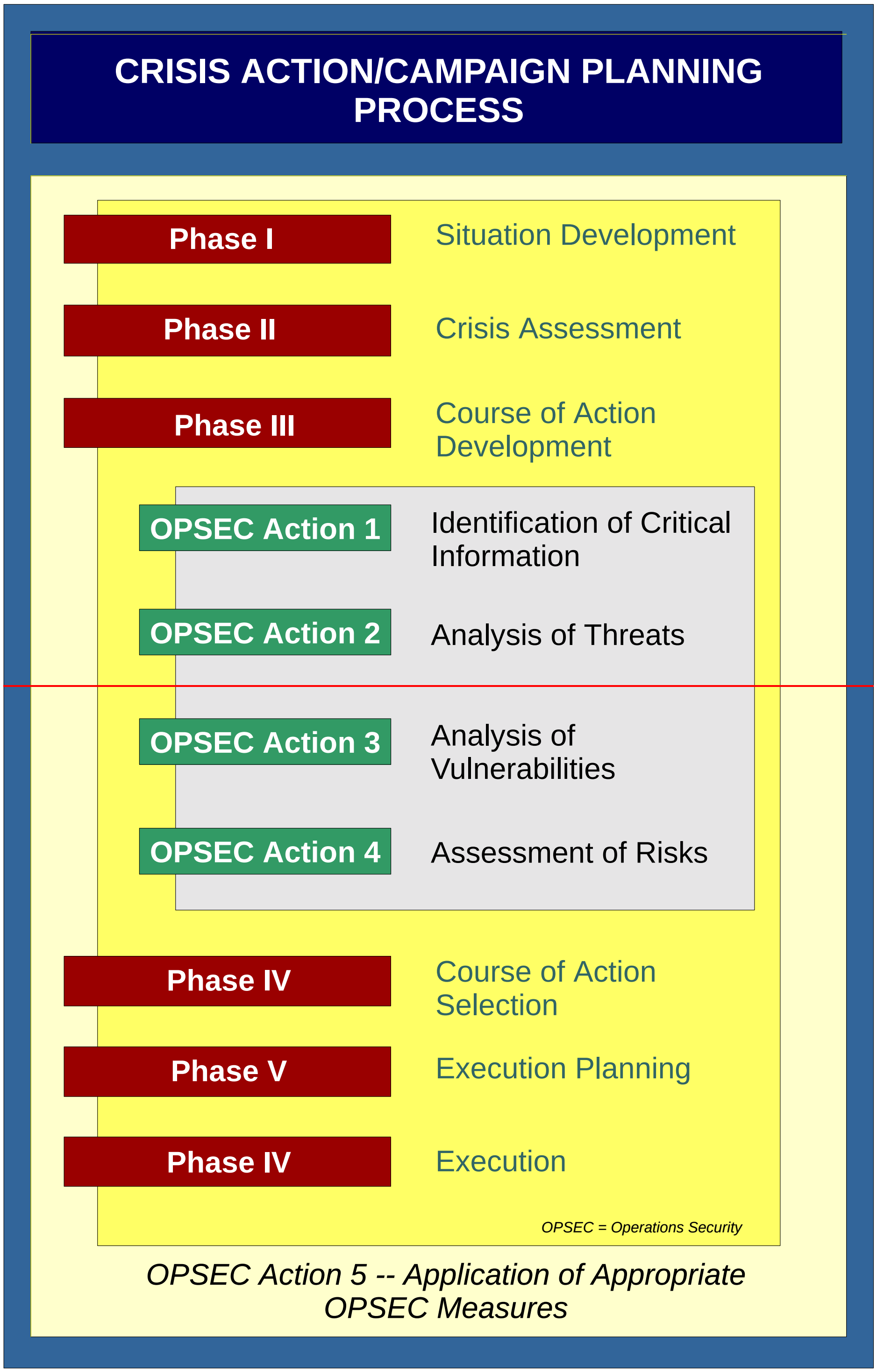
Phase IV — Plan Review

Phase V — Supporting Plans

OPSEC Action 5 -- Application of Appropriate OPSEC Measures (This relates to those measures intended to protect the plan prior to its being implemented)

*OPSEC = Operations Security

~~**Figure II-1. Deliberate Planning Process**~~



CRISIS ACTION/CAMPAIGN PLANNING PROCESS

Phase I Situation Development

Phase II Crisis Assessment

Phase III Course of Action Development

OPSEC Action 1 Identification of Critical Information

OPSEC Action 2 Analysis of Threats

OPSEC Action 3 Analysis of Vulnerabilities

OPSEC Action 4 Assessment of Risks

Phase IV Course of Action Selection

Phase V Execution Planning

Phase IV Execution

OPSEC = Operations Security

OPSEC Action 5 -- Application of Appropriate OPSEC Measures

~~**Figure II-2. Crisis Action/Campaign Planning Process**~~

5. OPSEC and Multinational Operations

a. US military operations often are **conducted with the armed forces of other nations** in pursuit of common objectives.

b. Multinational operations, both those that include combat and those that do not, are conducted with structure of an alliance or coalition.

(1) **An alliance** is a result of **formal agreements** between two or more nations for **broad, long-term objectives**. These alliance operations are combined operations, though in common usage combined often is used inappropriately as a synonym for all multinational operations.

(2) **A coalition** is an **ad hoc arrangement** between two or more nations for **common action**; for instance, the coalition that defeated Iraqi aggression against Kuwait in the Gulf War, 1990-1991.

c. Joint operations as part of an alliance or coalition **require close cooperation** among all forces and can serve to mass strengths, reduce vulnerabilities, and provide legitimacy. OPSEC measures that apply to joint operations are appropriate also for multinational situations.

d. Plans should be issued far enough in advance to allow sufficient time for member forces to conduct their own planning and rehearsals. Some alliance or coalition member forces may not have the planning and execution dexterity and flexibility characteristic of US forces. Accordingly, JFCs should ensure that the tempo of planning and execution does not exceed the capabilities of other member forces.

e. Intelligence. The collection, production, and dissemination of intelligence can be a major challenge. Alliance or coalition members normally operate separate intelligence systems in support of their own policy and military forces. JFCs should establish a system that optimizes each nation's contributions and provides member forces a common intelligence picture, tailored to their requirements and consistent with disclosure policies of member nations.

(1) **JFCs, in** accordance **with national directives, need to determine what intelligence may be shared** with the forces of other nations early in the planning process. The limits of intelligence sharing and the procedures for doing so should be included in agreements with multinational partners that are concluded after obtaining proper negotiating authority. Applying the OPSEC process to intelligence can assist in determining what information can be shared with coalition and what information requires greater protection.

(2) **The National Disclosure Policy provides initial guidance.** It promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definitions of terms, release arrangements, and other guidance. It also establishes

interagency mechanisms and procedures for the effective implementation of the policy. In the absence of sufficient guidance, JFCs should share only that information that is mission essential, affects lower-level operations, facilitates combat identification, and is perishable.

THE "BLACK HOLE": OPSEC DURING PLANNING

During the autumn of 1990, joint force air component commander (JFACC) planners merged the Air Force Component, Central Command (CENTAF) pre-deployment concept of operations with the INSTANT THUNDER concept to form the foundation for the Operation DESERT STORM plan for air operations.

Navy, USMC, and Army planners worked closely with Air Force (USAF) planners in August and September to draft the initial offensive air plan. In Riyadh, Navy Component, Central Command (NAVCENT), Marine Corps Component, Central Command (MARCENT), and Army Component, Central Command (ARCENT) were integral planning process members. Royal Air Force (RAF) planners joined the JFACC staff on 19 September.

CENTCOM's offensive air special planning group (SP6), in the Royal Saudi Air Force (RSAF) headquarters, was part of the JFACC staff and eventually became known as the "Black Hole" because of the extreme secrecy surrounding its activities. The Black Hole was led by a USAF brigadier general, reassigned from the *USS Lasalle* (AGF 3) where he had been serving as the deputy commander of Joint Task Force Middle East when Iraq invaded Kuwait. His small staff grew gradually to about 30 and included RAF, Army, Navy, USMC, and USAF personnel. By 15 September, the initial air planning stage was complete; the President was advised there were sufficient air forces to execute and sustain an offensive strategic air attack against Iraq, should he order one. However, because of operational security (OPSEC) concerns, most of CENTAF headquarters was denied information on the plan until only a few hours before execution.

**SOURCE: Final Report to Congress
Conduct of the Persian Gulf War, April 1992**

APPENDIX A

EXAMPLES OF OPSEC CRITICAL INFORMATION

This appendix provides general examples of critical information. Several generic military activities with some of their associated critical information are listed. These are only a few of the many types of military activities and their associated critical information.

1. Diplomatic Negotiations

a. Military capabilities (pretreaty and posttreaty)

b. Intelligence verification capabilities

c. Minimum negotiating positions

2. Politico-Military Crisis Management

a. Target selection

b. Timing considerations

c. Logistic capabilities and limitations d._Alert posture

3. Military Intervention

a._Intentions

b._Military capabilities

c._Forces assigned and in reserve

d._Targets

e._Timing

f._Logistic capabilities and constraints

g._Limitations

h._Third-nation support arrangements

i._Location of C4 nodes

j. Frequency and callsigns

4. Counterterrorism

a. Forces

b. Targets

c. Timing

d. Staging locations

e. Tactics

f. Ingress and egress methods/routes

g. Logistic capabilities and constraints

5. Open Hostilities

a. Force composition and disposition

b. Attrition and reinforcement

c. Targets

d. Timing

e. Logistic constraints

f. Location of critical C4~~2~~ nodes

6. Mobilization

a. Intent to mobilize before public announcement

b. Impact on military industrial base

c. Impact on civil economy

d. Transportation capabilities and limitations

7. Intelligence, Reconnaissance, and Surveillance

a. Purpose of collection

b._Targets of collection

c._Timing

d._Capabilities of collection assets

e._Processing capabilities

f._Unit requesting collection

g._Unit conducting collection

h._Communications capabilities

8. Peacetime Weapons and Other Military Movements

a._Fact of movement

b._Periodicity of movements

c._Origin and destination of equipment being moved

d._Capabilities and limitations of equipment being moved e._Extent of inventory of equipment being moved

9. Command Post Computer-Aided and Field Training Exercises

____a._Participating units

b._OPLAN, CONPLANs, or other contingencies that are being exercised

c._Command relationships

d._Command, control, communications, and computers connections and weaknesses

e._Logistic capabilities and limitations

10. Noncombatant Evacuation Operations (Hostile Environment)

a._Targets

b._Forces

c._Logistic constraints

d._Safe havens

e._Routes

f._Timing

11. Counterdrug Operations

a._Identity of military forces

b._Law Enforcement Agency (LEA) involvement

c._Military support to LEAs

d._Host-nation cooperation

e._Capabilities

f._Timing

g._Tactics

h._Logistic capabilities and constraints

Intentionally Blank

APPENDIX B

OPSEC INDICATORS

1. OPSEC Indicators

OPSEC indicators are those friendly actions and open sources of information that adversary intelligence ~~systems~~ can potentially detect, observe, or obtain and then interpret to derive friendly critical information.

2. Basic OPSEC Indicator Characteristics

An indicator's characteristics are those elements of an action or piece of information that ~~make it~~are potentially useful to an adversary. There are five major characteristics.

a. **Signature**

(1) A signature is the characteristic of an indicator that makes it identifiable or causes it to stand out. Key signature properties are uniqueness and stability. Uncommon or unique features reduce the ambiguity of an indicator and minimize the number of other indicators that must be observed to confirm a single indicator's significance.

(2) An indicator's signature stability, implying constant or stereotyped behavior, can allow an adversary to anticipate future actions. Varying the pattern of behavior

decreases the signature's stability and thus increases the ambiguity of the adversary's observations.

(3) Procedural features are an important part of any indicator signature and may provide the greatest value to an adversary. They identify how, when, and where the indicator occurs and what part it plays in the overall scheme of operations and activities.

b. **Associations**

(1) Association is the relationship of an indicator to other information or activities. It is an important key to an adversary's interpretation of ongoing activity. Intelligence analysts continuously compare their current observations with what has been seen in the past in an effort to identify possible relationships. For example, a distinctive piece of ground-support equipment known to be used for servicing strategic bombers might be observed at a tactical fighter base. An intelligence analyst could conclude that a strategic bomber presence has been or will be established there. The analyst will then look for other indicators associated with bombers to verify that conclusion.

(2) Another key association deals with continuity of actions, objects, or other indicators that may register as patterns to the observer or analyst. Such continuity may not be the result of planned procedures but may result instead from repetitive practices or sequencing to accomplish a goal. If, for example, the intensive generation of aircraft sorties is always preceded by a maintenance standdown to increase aircraft readiness,

detecting and observing the standdown may allow the adversary analyst or observer to predict the subsequent launch activity. Moreover, based on past patterns of the length of such standdowns, the analyst may be able to judge the scope of the sortie generation.

(3) Another type of association that is useful to intelligence analysts is organizational patterns. Military units, for example, are often symmetrically organized. Thus when some components are detected, others that are not readily apparent can be assumed to exist. For example, an intelligence analyst knows that a particular army's infantry battalions are organized with three infantry companies, a headquarters company, and a weapons company. If only the headquarters company and one infantry company are currently being detected, the presence of the other known battalion components will be strongly suspected. Thus in some situations, a pattern taken as a whole can be treated as a single indicator, simplifying the intelligence problem.

c. **Profiles**

(1) Each functional activity generates its own set of more-or-less unique signatures and associations. The sum of these signatures and associations is the activity's profile. An activity's profile is usually unique. Given enough data, intelligence analysts can determine the profile of any activity. Most intelligence organizations seek to identify and record the profiles of their adversary's military activities.

(2) The profile of an aircraft deployment, for example, may be unique to the

aircraft type or mission. This profile, in turn, has several subprofiles for the functional activities needed to deploy the particular mission aircraft (e.g., fuels, avionics, munitions, communications, air traffic control, supply, personnel, and transportation).

(3) The observation of a unique profile may sometimes be the only key that an intelligence analyst needs to determine what type of operation is occurring, thus minimizing the need to look harder for additional clues. Such unique profiles cut the time needed to make accurate intelligence estimates. As a result, profiles are the analytical tools.

d. **Contrasts**

(1) Contrasts are any differences that are observed between an activity's standard profile and its most recent or current actions. Contrasts are the most reliable means of detection because they depend on differences to established profiles. They also are simpler to use because they need only to be recognized, not understood.

(2) Deviations from normal profiles will normally attract the interest of intelligence analysts. They will want to know why there is a change and attempt to determine if the change means anything significant.

(3) In the previous example of the distinctive bomber-associated ground support equipment at a fighter base, the intelligence observer might ask the following questions:

(a) Have bombers been deployed at fighter bases before? At this particular fighter base? At several fighter bases simultaneously?

(b) If there have been previous bomber deployments, were they routine or did they occur during some period of crisis?

(c) If previous deployments have been made to this base or other fighter bases, how many bomber aircraft were deployed?

(d) What actions occurred while the bombers were deployed at the fighter bases?

(e) What is happening at other fighter and bomber bases? Is this an isolated incident or one of many changes to normal activity patterns?

(4) Although the detection of a single contrast may not provide intelligence analysts with a total understanding of what is happening, it may result in increased intelligence collection efforts against an activity.

e. **Exposure**

(1) Exposure refers to when and for how long an indicator is observed. The

duration, repetition, and timing of an indicator’s exposure can affect its relative importance and meaning. Limiting the duration and repetition of exposure reduces the amount of detail that can be observed and the associations that can be formed.

(2) An indicator (object or action) that appears over a long period of time will be assimilated into an overall profile and assigned a meaning. An indicator that appears for a short time and does not appear again may, if it has a high interest value, persist in the adversary intelligence database or, if there is little or no interest, fade into the background of insignificant anomalies. An indicator that appears repeatedly will be studied carefully as a contrast to normal profiles.

(3) Because of a short exposure time, the observer or analyst may not detect key characteristics of the indicator the first time it is seen, but he can formulate questions and focus collection assets to provide answers if the indicator is observed again.

(4) Repetition of the indicator in relationship to an operation, activity, or exercise will add it to the profile even if the purpose of the indicator is not understood by the adversary. Indicators limited to a single isolated exposure are difficult to detect and evaluate.

3. Examples of Indicators

The following paragraphs provide examples of indicators that are associated with selected military activities and information. This short list only scratches the surface of the almost infinite sources of indicators associated with the wide range of US military operations and activities that could be exploited by an adversary. This list is designed primarily to stimulate thinking about what kinds of actions can convey indicators that betray critical information for specific friendly operations or activities.

a. **Indicators of General Military Force Capabilities**

(1) The presence of unusual type units for a given location, area, or base.

(2) Friendly reactions to adversary exercises or actual hostile actions.

(3) Actions, information, or material associating Reserve Components with specific commands or units (e.g., mobilization and assignment of Reserve personnel to units).

(4) Actions, information, or material indicating the levels of unit manning as well as the state of training and experience of personnel assigned.

(5) Actions, information, or material revealing spare parts availability for equipment or systems.

(6) Actions, information, or material indicating equipment or system reliability

(e.g., visits of technical representatives or special repair teams).

(7) Movement of aircraft, ships, and ground units in response to friendly sensor detections of hostile units.

(8) Actions, information, or material revealing tactics, techniques, and procedures employed in different types of training exercises or during equipment or system operational tests and evaluations.

(9) Stereotyped patterns in performing the organizational mission that reveal the sequence of specific actions or when they are accomplished.

b. **Indicators of General Command and Control (C2) Capabilities**

(1) Actions, information, or material providing insight into the volume of orders and reports needed to accomplish tasks.

(2) Actions, information, or material showing unit subordination for deployment, mission, or task.

(3) Association of particular commanders with patterns of behavior under stress or in varying tactical situations.

(4) Information revealing problems of coordination between the commander's staff elements.

(5) In exercises or operations, indications of the period between the occurrence of a need to act or react and the action taking place, of consultations that occur with higher commands, and of the types of actions initiated.

(6) Unusual actions with no apparent direction reflected in communications.

c. **General Indicators from Communications Usage**

(1) Alert and maintenance personnel using handheld radios or testing aircraft or vehicle radios.

(2) Establishing new communications nets. These might reveal entities that have intrinsic significance for the operation or activity being planned or executed. Without conditioning to desensitize adversaries, the sudden appearance of new communications nets could prompt them to implement additional intelligence collection to discern friendly activity more accurately.

(3) Suddenly increasing traffic volume or, conversely, instituting radio silence when close to the time of starting an operation, exercise, or test. Without conditioning, unusual surges or periods of silence may catch adversaries' attention and, at a minimum,

prompt them to focus their intelligence collection efforts.

(4) Using static call signs for particular units or functions and unchanged or infrequently changed radio frequencies. This usage also allows adversaries to monitor friendly activity more easily and add to their intelligence data base for building an accurate appreciation of friendly activity.

(5) Using stereotyped message characteristics that indicate particular types of activity that allow adversaries to monitor friendly activity more easily.

(6) Requiring check-in and checkout with multiple control stations before, during, and after a mission (usually connected with air operations).

d. **Sources of Possible Indicators for Equipment and System Capabilities**

(1) Unencrypted emissions during tests and exercises.

(2) Public media, particularly technical journals.

(3) Budget data that provide insight into the objectives and scope of a system research and development effort or the sustainability of a fielded system.

(4) The equipment or system hardware itself.

(5) Information on test and exercise schedules that allows adversaries to better plan the use of their intelligence collection assets.

(6) Deployment of unique units, targets, and sensor systems to support tests associated with particular equipment or systems.

(7) Unusual or visible security imposed on particular development efforts that highlight their significance.

(8) Information indicating special manning for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract.

(9) Notices to mariners and airmen that might highlight test areas.

(10) Stereotyped use of location, procedures, and sequences of actions when preparing for and executing test activity for specific types of equipment or systems.

(11) Use of advertisements indicating that a company has a contract on a classified system or component of a system, possesses technology of military significance, or has applied particular principles of physics and specific technologies to sensors and the guidance components of weapons.

e. **Indicators of Preparations for Operations or Activities**. Many indicators may reveal data during the preparatory, as compared to the execution, phase of operations or activities. Many deal with logistic activity.

(1) Provisioning of special supplies for participating elements.

(2) Requisitioning unusual volumes of supply items to be filled by a particular date.

(3) Increasing prepositioning of ammunition, fuels, weapon stocks, and other classes of supply.

(4) Embarking special units, installing special capabilities, and preparing unit equipment with special paint schemes.

(5) Procuring large or unusual numbers of maps and charts for specific locations.

(6) Making medical arrangements, mobilizing medical personnel, stockpiling pharmaceuticals and blood, and marshalling medical equipment.

(7) Focusing friendly intelligence and reconnaissance assets against a particular area of interest.

(8) Requisitioning or assigning increased number of linguists of a particular language or group of languages from a particular region.

(9) Initiating and maintaining unusual liaison with foreign nations for support.

(10) Providing increased or tailored personnel training.

(11) Holding rehearsals to test concepts of operation.

(12) Increasing the number of trips and conferences for senior officials and staff members.

(13) Sending notices to airmen and mariners and making airspace reservations.

(14) Arranging for tugs and pilots.

(15) Requiring personnel on leave or liberty to return to their duty locations.

(16) Having unusual off-limits restrictions.

(17) Preparing units for combat operations through equipment checks as well as operational standdowns in order to achieve a required readiness level for equipment and

personnel.

(18) Making billeting and transportation arrangements for particular personnel or units.

(19) Taking large-scale action to change mail addresses or arrange for mail forwarding.

(20) Posting such things as supply delivery, personnel arrival, transportation, or ordnance loading schedules in a routine manner where personnel without a need-to-know will have access.

(21) Storing boxes or equipment labeled with the name of an operation or activity or with a clear unit designation outside a controlled area.

(22) Employing uncleared personnel to handle materiel used only in particular types of operations or activities.

(23) Providing unique or highly visible physical security arrangements for loading or guarding special munitions or equipment.

(24) Requesting unusual or increased meteorological, oceanographic, or ice information for a specific area.

(25) Setting up a wide-area network (WAN) over commercial lines.

f. **Sources of Indicators During the Execution Phase**

(1) Unit and equipment departures from normal bases.

(2) Adversary radar, sonar, or visual detections of friendly units.

(3) Friendly unit identifications through COMSEC violation or physical observation of unit symbology.

(4) Force composition and tracks or routes of advance that can be provided by emissions from units or equipment and systems that provide identifying data.

(5) Stereotyped procedures; static and standard ways of composing, disposing, and controlling strike or defensive elements against particular threats; and predictable reactions to enemy actions.

(6) Alert of civilians in operational areas.

(7) Trash and garbage dumped by units or from ships at sea that might provide unit identifying data.

(8) Transportation of spare parts or personnel to deploying or deployed units or via commercial aircraft or ship.

(9) Changes in oceanography high frequency facsimile transmissions.

(10) Changes in the activity over WAN.

g. **Indicators of Post engagement Residual Capabilities**

(1) Repair and maintenance facilities schedules.

(2) Urgent calls for maintenance personnel.

(3) Movement of supporting resources.

(4) Medical activity.

(5) Unusual resupply and provisioning of an activity.

(6) Assignment of new units from other areas.

(7) Search and rescue activity.

(8) Personnel orders.

(9) Discussion of repair and maintenance requirements in unsecure areas.

(10) Termination or modification of procedures for reporting of unclassified meteorological, oceanographic, or ice information.

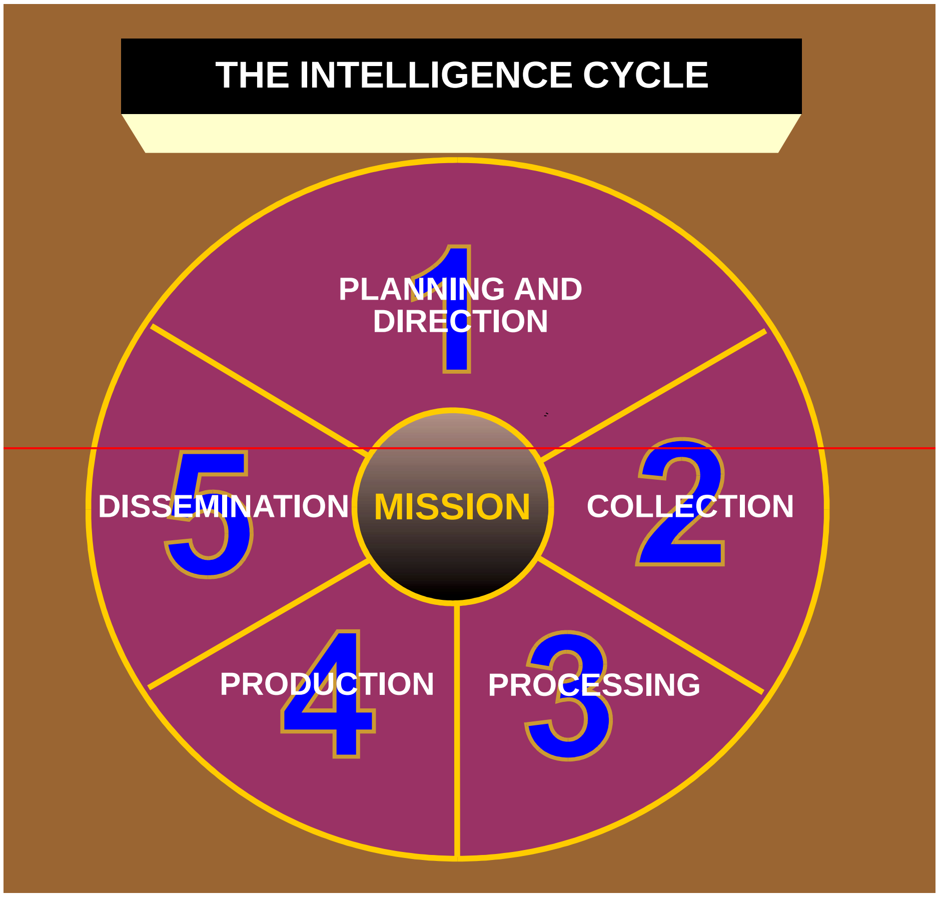
Intentionally Blank

~~APPENDIX B~~

~~THE INTELLIGENCE THREAT~~

~~1. Introduction~~

~~Adversaries and potential adversaries collect and analyze information about US military operations in order to determine current capabilities and future intentions. To perform this function, most adversaries have created intelligence organizations and systems. The capabilities and levels of sophistication of these threats differ greatly, but they all share certain core characteristics. The most important of these are how intelligence is developed and how it is collected. This appendix will describe those characteristics.~~



~~Figure B-1. The Intelligence Cycle~~

~~2. The Intelligence Cycle~~

~~All intelligence systems follow a process. This process begins with a consumer (a commander or decision maker) requesting answers to certain questions and ends with the intelligence system providing those answers. Figure B-1 illustrates a typical intelligence cycle (in this case, the intelligence cycle described in Joint Pub 2-0, “Joint Doctrine for Intelligence Support to Operations”). Understanding the concept of the intelligence cycle is basic to understanding the total adversary intelligence threat to friendly operations in general and the specific threat to the critical information that OPSEC seeks to protect.~~

~~a. Planning and Direction~~

- ~~Decision makers task their intelligence systems to collect and assess information about their adversaries and potential adversaries. These information requirements are the basis for intelligence collection, evaluation, and reporting.~~

- ~~These information requirements will normally include any information that would allow the decision maker to better understand an adversary's goals, intentions, current capabilities, strengths, and weaknesses. At the operational and strategic levels of war, decision makers will want to know what their adversary counterparts think; how they make their decisions; and their social, cultural, economic, and political beliefs and habits.~~

- ~~Intelligence specialists take the decision maker's information requirements and turn them into specific intelligence taskings.~~

~~b. Collection~~

- ~~After determining the taskings, the intelligence system will evaluate the currency and amount of information already at hand. If more or newer information is needed, collection requirements will be submitted to the appropriate collection resources.~~

~~Information may be collected either overtly or clandestinely.~~

~~•• Overt collection may include such activities by military attaches assigned to embassies and the review of available open-source information.~~

~~•• Clandestine collection acquires information while concealing the collection effort and consists of espionage and technical means such as signals and imagery intelligence.~~

~~c. Processing. Collected information must be processed into a form that is suitable for the production of intelligence. For example, imagery film must be developed and signals must be processed before they can be evaluated, analyzed, and interpreted for significance.~~

~~d. Production~~

~~• The still raw intelligence is evaluated for accuracy, reliability, and credibility. It is compared for consistency with known data and examined for meaningful associations by analyzing it against its historical background. It is combined with other information. The information is analyzed, interpreted, and prepared for presentation to the consumer. There are numerous types of intelligence products ranging from informal briefings to multivolume written studies.~~

- ~~Generally, every product attempts to address the questions, “What is the adversary doing now?" and "What is it going to do next?” In many cases, because of inadequate collection or insufficient time for processing and analysis, intelligence analysts will not be able to provide unambiguous answers to those questions. This phase of the intelligence cycle is still more art than science.~~

~~e. Dissemination. In this step, the product is delivered to the consumer. There are as many forms of delivery as there are products and consumers. Automated means are becoming increasingly important in many intelligence systems.~~

~~3. Intelligence Sources~~

~~a. Human Intelligence (HUMINT). HUMINT uses people to gain information that is often inaccessible by other collection means. Although it is the oldest and most basic form of intelligence collection, HUMINT remains significant because it is often the only source with direct access to the opponent’s plans and intentions. Clandestine HUMINT collection is done in a fashion that maintains the secrecy of the collection operation.~~

~~b. Imagery Intelligence (IMINT)~~

- ~~IMINT is derived from visual photography, infrared sensors, lasers, electro-optics, and radar sensors. IMINT systems can operate from land, sea, air, and/or space platforms. Imagery equipment is being improved constantly, and combinations of~~

~~sensors are being used to enhance the quality and timeliness of the intelligence product.~~

- ~~An increasing number of countries are starting to use photo reconnaissance satellites. In addition to being a major strategic collection capability, they are becoming an increasingly important operational and tactical capability. The traditional airborne IMINT platforms remain an important capability for those countries without access to satellite imagery.~~

~~c. Signals Intelligence (SIGINT). SIGINT is derived from communication (COMINT), electronics (ELINT), and foreign instrumentation signals (FISINT).~~

- ~~COMINT is technical and intelligence information derived from foreign communications by other than the intended recipients. Prime COMINT sources include clear voice (nonencrypted) telephone and radio communications and unencrypted computer-to-computer data communications.~~

- ~~ELINT is technical or geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Radars are the primary ELINT source.~~

- ~~FISINT is derived from the intercept and analysis of electronically transmitted data containing measured parameters of performance, such as a ballistic missile's~~

~~performance during a test flight.~~

~~d. Measurement and Signature Intelligence (MASINT). MASINT is scientific and technical intelligence obtained by the quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same. MASINT includes other intelligence sources such as acoustical intelligence, laser intelligence, and nuclear intelligence.~~

~~e. Open Source Intelligence (OSINT). OSINT is information of potential intelligence value that is available to the general public. OSINT is available from such sources as the news media, public affairs announcements, unclassified government documents and publications, public hearings, and contracts and contract-related material.~~

~~f. Technical Intelligence (TECHINT). TECHINT is derived from the exploitation of foreign materiel. It results from the analysis of captured or otherwise obtained foreign equipment.~~

~~Intentionally Blank~~

APPENDIX C

OPERATIONS SECURITY MEASURES

The following OPSEC measures are offered as a guide only. Development of specific OPSEC measures is as varied as the specific vulnerabilities they are designed to offset.

1. Operational and Logistic Measures

a. Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations or activities in terms of time, place, event sequencing, formations, and C2 arrangements.

b. Employ force dispositions and C2 control arrangements that conceal the location, identity, and command relationships of major units.

c. Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.

d. Transport supplies and personnel to combat units in a way that conceals the location and identity of the combat units.

e. Operate aircraft at low altitude to avoid radar detection.

f. Operate to minimize the reflective surfaces that units or weapon systems present to radars and sonars.

g. Use darkness to mask deployments or force generation.

h. Approach an objective "out of the sun" to prevent detection.

2. Technical Measures

Limit computer email messages to non-military activities. Do not provide operational information in email messages.

a. Prepare for CNA. Place vital operational information on disk.

b. Use encryption to protect voice, data, and video communications.

c. Use radio communications emission control, low-probability-of-intercept techniques and systems, traffic flow security, padding, flashing light or flag hoist, ultra high frequency relay via aircraft, burst transmission technologies, secure phones, landline, and couriers. Limit use of high frequency radios and directional super-high frequency transponders.

d. Control radar emission, operate at reduced power, operate radars common to many units, assign radar guard to units detached from formations or to air early warning aircraft, and use anechoic coatings.

e. Mask emissions or forces from radar or visual detection by use of terrain (such as mountains and islands).

f. Maintain sound silence or operate at reduced power, proceed at slow speeds, turn off selected equipment, and use anechoic coatings.

g. Use screen jamming, camouflage, smoke, background noise, added sources of heat or light, paint, or weather.

3. Administrative Measures

a. Limit telephone conversation to non-military activities.

b. Avoid bulletin board, plan of the day, or planning schedule notices that reveal when events will occur.

c. Conceal budgetary transactions, supply requests and actions, and arrangements for services that reveal preparations for activity.

d. Conceal the issuance of orders, the movement of specially qualified personnel to units, and the installation of special capabilities.

e. Control trash and garbage dumping or other housekeeping functions to conceal the locations and identities of units.

f. Follow normal leave and liberty policies to the maximum extent possible before an operation starts in order to preserve a sense of normalcy.

g. Ensure that personnel discretely prepare for their families' welfare in their absence and that their families are sensitized to their potential abrupt departure.

4. OPSEC and Military Deception

a. OPSEC used in conjunction with military deception can assist commanders to protect key elements of operations and ensure mission success. ~~Military deception can be an effective OPSEC measure, provided that prior coordination is accomplished when actions will affect other commanders.~~ OPSEC, with ~~M~~military deception, can be used to facilitate the following.

(1) Cause adversary intelligence to fail to target friendly activity; collect against targeted tests, operations, exercises, or other activities; or determine through analysis vital capabilities and characteristics of systems and vital aspects of policies, procedures,

doctrine, and tactics.

(2) Create confusion about, or multiple interpretations of, vital information obtainable from open sources.

(3) Cause a loss of interest by foreign and random observers in test, operation, exercise, or other activity.

(4) Convey inaccurate locating and targeting information to opposing forces.

b. In accordance with ~~CJCSI 3211.01A~~JP 3-58, *Joint Doctrine for Joint Military Deception*, commanders are authorized to conduct military deception:

(1) To support OPSEC during the preparation and execution phases of normal operations, provided that prior coordination is accomplished for actions that will affect other commanders~~; and~~.

(2) When the commander's forces are engaged or are subject to imminent attack.

5. OPSEC, Physical Destruction and EW

During hostilities, use physical destruction and electronic attack against the adversary's ability to collect and process information. IO~~C2W~~ actions that ~~can be~~are used in support of OPSEC include strikes against an adversary’s satellites, SIGINT sites, radars, fixed sonar installations, reconnaissance aircraft, and ships.

APPENDIX D

PROCEDURES FOR OPSEC ~~SURVEYS~~ASSESSMENTS

1. General

a. The purpose of an OPSEC ~~survey~~assessment is to thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists.

b. Ideally, the operation or activity being ~~surveyed~~assessed ~~will be using~~uses OPSEC measures to protect its critical information. The OPSEC ~~survey~~assessment is used ~~as a check on how~~ to verify the effectiveness of ~~the~~OPSEC measures~~ are~~. The ~~survey~~assessment will determine if ~~the~~ critical information identified during ~~the~~ OPSEC planning process is being protected.

c. An ~~survey~~assessment cannot be conducted until after an operation or activity has at least identified its critical information. Without a basis of ~~identified~~ critical information, there can be no specific determination that actual OPSEC vulnerabilities exist.

2. Uniqueness

a. Each OPSEC ~~survey~~assessment is unique. ~~Survey~~Assessments differ in the nature of the information requiring protection, the adversary collection capability, and the environment of the activity to be ~~surveyed~~assessed.

b. In combat, an ~~survey~~assessment’s emphasis must be on identifying operational indicators that signal friendly intentions, capabilities, and/or limitations and that ~~will~~ permits the adversary to counter friendly operations or reduce their effectiveness.

c. In peacetime, ~~survey~~assessments generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit tests, drills, practice alerts, and major exercises, are of great interest to a ~~-~~potential adversary because they provide insight into friendly readiness, plans, crisis procedures, and C2 capabilities that enhance that adversary’s long-range planning.

3. OPSEC ~~Survey~~Assessments Versus Security Inspections

a. OPSEC ~~survey~~assessments are different from security evaluations or inspections. An ~~survey~~assessment attempts to produce an adversary’s view of the operation or activity being ~~surveyed~~assessed. A security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations.

b. ~~Survey~~Assessments are always planned and conducted by the organization responsible for the operation or activity that is to be ~~surveyed~~assessed. Inspections may be conducted without warning by outside organizations.

c. OPSEC ~~survey~~assessments are not a check on the effectiveness of an organization’s security programs or its adherence to security directives. In fact, ~~survey~~assessment teams will be seeking to determine if any security measures are creating OPSEC indicators.

d. ~~Survey~~Assessments are not punitive inspections, and no grades or evaluations are awarded as a result of them. ~~Survey~~Assessments are not designed to inspect individuals but are employed to evaluate operations and systems used to accomplish missions.

e. To obtain accurate information, an ~~survey~~assessment team must depend on positive cooperation and assistance from the organizations participating in the operation or activity being ~~surveyed~~assessed. If team members must question individuals, observe activities, and otherwise gather data during the course of the ~~survey~~assessment, they will inevitably appear as inspectors, unless this nonpunitive objective is made clear.

f. Although reports are not provided to the ~~surveyed~~assessed unit’s higher headquarters, OPSEC ~~survey~~assessment teams may forward to senior officials the lessons learned on a nonattribution basis. The senior officials responsible for the operation or activity then decide to further disseminate the ~~survey~~assessment’s lessons learned.

4. Types of ~~Survey~~Assessments

There are two basic kinds of OPSEC ~~survey~~assessments; command and formal.

a. A command ~~survey~~assessment is performed using only command personnel and concentrates on events within the particular command.

b. A formal ~~survey~~assessment requires an ~~survey~~assessment team composed of members from inside and outside the command and will normally cross command lines (after prior coordination) to ~~survey~~assessment supporting and related operations and activities. Formal ~~survey~~assessments are initiated by a letter or message stating the subject of the ~~survey~~assessment, naming the team leader and members, and indicating when the ~~survey~~assessment will be conducted. Commands, activities, and locations to be visited may also be listed, with the notation that the team may visit additional locations if required during the field portion of the ~~survey~~assessment.

c. Both types of ~~survey~~assessments follow the same basic sequence and procedures that are established in the annexes to this appendix.

5. ~~Survey~~Assessment Execution

a. Careful prior planning, thorough data collection, and thoughtful analysis of the results are the key phases of an effective OPSEC ~~survey~~assessment.

b. The following annexes describe the three phases of an OPSEC ~~survey~~assessment.

Intentionally Blank

ANNEX A TO APPENDIX D

OPSEC ~~SURVEY~~ASSESSMENT PLANNING PHASE

Preparations for an OPSEC ~~survey~~assessment ~~must~~ begins well in advance of the field ~~survey~~assessment phase. The required lead time will depend on the nature and complexity of the operation and activities ~~to be survey~~assessed (combat operations, peacetime operational activity, or other type of operation). Sufficient time ~~must be~~ allot~~ted~~s in the planning phase for a thorough review of pertinent documentation, for formal and informal coordination and discussions, and for ~~the~~ careful preparation of functional outlines. The following actions normally make up the planning phase.

1. Determine the Scope of the Assessment

The scope of the ~~survey~~assessment ~~should be~~is defined at the start of the planning phase and ~~be~~ limited to manageable proportions. Limitations ~~will be~~ are imposed by geography, time, units to be observed, funding, and other practical matters.

2. Select Team Members

a. Regardless of the ~~survey~~assessment's external or internal focus, the team should contain multidisciplined expertise. ~~Survey~~Assessment team members should be selected for their analytical, observational, and problem-solving abilities.

b._Since ~~survey~~assessments are normally oriented to operations, the senior member should be selected from the operations (or equivalent) staff of the commander responsible for conducting the ~~survey~~assessment.

c._Typical team members would represent the functional areas of intelligence, security, communications, logistics, plans, information assurance, public affairs, and administration. When appropriate, specialists from other functional areas, such as transportation ~~and public affairs,~~ will participate.

d._When communications monitoring is planned as part of the ~~survey~~assessment, the monitoring group's leader should be designated as a member of the OPSEC ~~survey~~assessment team. Team members ~~must be~~are brought together early in the planning phase to ensure timely, thorough accomplishment of the tasks outlined below.

3. Become Familiar with ~~Survey~~Assessment Procedures

Designating team members with ~~survey~~assessment experience is advantageous, but is often not possible. In such cases, team members will require familiarization with ~~survey~~assessment procedures.

4. Determine the Adversary Intelligence Threat

The adversary threat to the activities to be ~~survey~~assessed ~~must be~~are evaluated carefully and realistically. An all-source threat assessment should comprehensively address the adversary intelligence capability, taking into account, not only the adversary's collection capabilities, ~~(see Appendix B, "The Intelligence Threat")~~ but also the adversary's ability to exploit the collection results in a timely manner.

5. Understand the Operation or Activity ~~to be Survey~~Assessed

The team members' thorough understanding of the operation or activity to be ~~survey~~assessed is crucial to ensuring the success of subsequent phases of the ~~survey~~assessment. Team members should become familiar with the operation plans, orders, standard operating procedures, or other directives bearing on the ~~survey~~assessed operation or activity. This initial review familiarizes team members with the mission and concept of operation and identifies most of the organizations participating in the ~~survey~~assessed activity (others may be identified as the ~~survey~~assessment progresses).

6. Conduct Empirical Studies

a. Empirical studies simulate aspects of the adversary intelligence threat and support vulnerability findings. These studies also help the ~~survey~~assessment team identify vulnerabilities that cannot be determined through interviews and observation. The results of these studies are useful to the ~~survey~~assessment team during the field or analytic phase of the ~~survey~~assessment.

b._An example of an empirical study is signals monitoring. Computer modeling or other laboratory simulations of the enemy threat, the impact on friendly forces, and the impact of implementing defensive measures may also be useful to the ~~survey~~assessment team. These studies are usually performed by ~~-~~organizations external to the one sponsoring the OPSEC ~~survey~~assessment team. Arrangements for their use should be made as far in advance of the ~~survey~~assessment as possible.

7. Develop a Functional Outline

a._A basic OPSEC ~~survey~~assessment technique involves the construction of a chronology of events that are expected to occur in the ~~survey~~assessed operation or activity. Events are assembled sequentially, thus creating a timeline that describes in detail the activities or plans of an operation or activity.

b._Chronologies should first be constructed for each separate functional area, such as operations, communications, logistics, or administration. This functional approach aids the team members in defining their separate areas of inquiry during the field or data collection phase of the ~~survey~~assessment. Later, the functional outlines can be correlated with each other to build an integrated chronology of the entire operation or activity. ~~ee Tab A, Composite OPSEC Profile for Combat Operations.~~

c._After the chronology is assembled, vulnerabilities can be identified in light of the known or projected threat.

d._During the initial review of ~~operation plans~~ OPLANS, orders, and procedures, individual team members can begin to develop functionally oriented outlines for their areas of interest. Initially, the outlines ~~will be~~are skeletal projections, in a narrative, table, or graph format, of what is expected to occur in the chronology for a particular functional area (see Tabs B through F).

e._Such projections can serve as planning aids for the subsequent field ~~survey~~assessment phase. For example, units and facilities associated with each of the events ~~can be~~are identified and geographically grouped to aid in planning the travel itinerary of team members during the field ~~survey~~assessment. Collectively, the initial functional outlines provide a basis for planning the field ~~survey~~assessment phase and constitute a basis for observation and interviews.

g._During the field ~~survey~~assessment phase, team members will acquire additional information through observation, interviews, and other data-collection techniques, enabling further development and refinement of the functional outlines.

h._Collectively, the outlines project a time-phased picture of the events associated with the planning, preparation, execution, and conclusion of the operation or activity. The outlines also provide an analytic basis for identifying events and activities that are vulnerable to adversary exploitation.

8. Determine Preliminary Friendly Vulnerabilities

After the adversary intelligence threat and the OPSEC indicators are determined, a subjective evaluation must be made of the potential friendly vulnerabilities. A vulnerability (e.g., a detectable, exploitable event) may or may not carry a security classification at the time of its identification, but such preliminary vulnerabilities must be protected from disclosure by administrative or security controls. These preliminary friendly vulnerabilities ~~will be~~are refined in later stages of the OPSEC ~~survey~~assessment.

9. Announce the ~~Survey~~Assessment

a. After team members are selected and are familiar with the operation or activity to be ~~survey~~assessed, the organization conducting the ~~survey~~assessment should inform its subordinate and supporting organizations that a ~~survey~~assessment will be conducted so that preparations can be made to support the team during the field ~~survey~~assessment phase.

b. The following information should be included:

(1) ~~Survey~~Assessment purpose and scope.

(2) List of team members and their clearances.

(3) List of required briefings and orientations.

(4) Timeframe involved.

(5) Administrative support requirements.

(6) Signals security (SIGSEC) monitoring support requirements (if needed).

Intentionally Blank

TAB A TO ANNEX A TO APPENDIX D

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE

FOR INTELLIGENCE COLLECTION OPERATIONS

The completed profile reflects a picture of the intelligence collection effort. Intelligence collection is normally one of the first functional areas to present indicators of an impending operation or activity.

1. Planned Event Sequence. See intelligence collection plan prepared by intelligence staff element.

2. Actual Event Sequence. Observe events in the operation center.

3. Analysis. Determine any OPSEC vulnerabilities. If vulnerabilities exist, determine whether they exist because of an error or because they are the result of normal procedures.

4. Examples of Typical Indicators

a. Appearance of specialized intelligence collection equipment in a particular area.

b. Increased traffic on intelligence communications nets.

c. Increased manning levels and/or work hours in intelligence facilities.

d. Increased research activity by known intelligence activities and personnel in libraries and electronic databases.

e. Increased activity of friendly agent nets.

f. Increased levels of activity by airborne intelligence systems.

g. Alterations in the orbits of intelligence satellites.

h. Interviews with nongovernmental subject matter experts conducted by intelligence personnel.

i. Requests for maps and other topographic material.

TAB B TO ANNEX A TO APPENDIX D

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR LOGISTICS

The completed logistic profile presents a picture of logistic activities conducted in preparation for an impending operation. As in the administration function, the long lead time for some preparations gives early warning of forthcoming operations if events are compromised.

1. **Planned Event Sequence**. See logistic annex to OPLAN.

2. **Actual Event Sequence.** Observation, interviews.

3. **Analysis.** As in other functional areas.

4. **Examples of Typical Indicators**

a. Special equipment issue.

b. Pre-positioning of equipment and supplies.

c. Increased weapons and vehicle maintenance.

d. Petroleum, oils, and lubricants stockpiling.

e. Upgrading lines of communications.

f. Ammunition stockpiling.

g. Delivery of special munitions and uncommon munitions (discloses possible nature of operation).

h. Arrival of new logistic units and personnel.

i. Increased requisition of supplies.

j. Increased traffic on logistics communications nets.

k. Changes in normal delivery patterns.

TAB C TO ANNEX A TO APPENDIX D

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR COMMUNICATIONS

____In addition to presenting a picture of its own functional area, friendly communications also reflect all other functional areas. Communications surveillance and communications logs for all functional nets are important tools in evaluating this functional area as well as other functions involved.

____1. Planned Event Sequence. OPLAN, operation order (OPORD), signal operation instructions, or standing signal instruction.

____2. Actual Event Sequence. Communications monitoring and communications logs.

____3. Analysis. As in other functional areas.

____4. Examples of Typical Indicators

____a._Increased radio, teletype, and telephone traffic.

____b._Increased communications checks.

____c._Appearance of new stations in net.

____d. New frequency and call-sign assignments.

____e. New codes and authenticators.

____f. Radio silence.

____g. Changing call-up patterns.

____h. Use of maintenance frequencies to test equipment.

____i. Communications command post exercises.

____j. Appearance of different cryptographic equipment and materials.

________k. Unclassified network activity.

TAB D TO ANNEX A TO APPENDIX D

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR OPERATIONS

The completed profile of operational activities reflects events associated with tactical combat units as they prepare for an operation.

1. Planned Event Sequence. OPLAN, OPORD, ~~standing~~ standard operating procedure (SOP).

2. Actual Event Sequence. Observations, reports, messages, interviews.

3. Analysis. As in other functional areas.

4. Examples of Typical Indicators

a. Rehearsals and drills.

b. Special-tactics refresher training.

c. Appearance of special-purpose units (bridge companies, forward air controllers, pathfinders, mobile weather units).

____d._Pre-positioning of artillery and aviation units.

____e._Artillery registration in new objective area.

____f._Complete cessation of activity in area in which reconnaissance activity previously took place.

____g._Appearance of new attached units.

____h._Issuance of new equipment.

____i._Changes in major unit leadership.

____j._Repositioning of maneuver units.

TAB E TO ANNEX A TO APPENDIX D

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE

FOR ADMINISTRATION AND SUPPORT

____The completed profile of administrative and support events shows activities taking place before the operation, thereby giving advance warning.

____1. Planned Event Sequence. Derive from unit SOPs and administrative orders.

____2. Actual Event Schedule. Observations and interviews.

____3. Analysis. As in other functional areas.

____4. Examples of Typical Indicators

____a._Release of groups of personnel or complete units for personal affairs.

____b._Runs on exchanges for personal articles, cleaning, and other items.

____c._Changes to wake-up and ~~mess~~dining schedules.

____d._Changes to mailing addresses.

____e._New unit designators on mail.

____f._Emergency personnel requisitions and fills for critical skills.

____g._Medical supply stockpiling.

____h._Emergency recall of personnel on pass and leave.

ANNEX B TO APPENDIX D

FIELD ~~SURVEY~~ASSESSMENT PHASE

As noted previously, data collection begins in the planning phase with a review of associated documentation. During the field ~~survey~~assessment phase, interviews with personnel directly involved in the operation, together with observations and document collection, are the primary means of data collection. The following actions are normally accomplished during the field ~~survey~~assessment phase.

1. Commanding Briefing on Operation to be Assessed

This briefing is presented to the OPSEC ~~survey~~assessment team by the command directing the forces or assets involved in the operation or activity being ~~surveyed~~assessed. The purpose of the briefing is to provide the ~~survey~~assessment team with an overview of the operation from the command's point of view. Team members should use this opportunity to clarify remaining questions about the information developed in the planning phase.

2. OPSEC Assessment Team Briefing

This briefing is presented by the chief of the ~~survey~~assessment team to the commander and principal staff officers of the ~~surveyed~~assessed organization. The briefing may be either a formal presentation or an informal discussion. The objective is to inform the commander and the staff of how the ~~survey~~assessment will be conducted. The briefing ~~should~~ includes a summary of the hostile threat and the vulnerability assessment developed during the planning phase. The staff should be asked to comment on the validity of this assessment. Results of previous OPSEC ~~survey~~assessments of similar activities may be summarized.

3. Data Collection and Functional Outline Refinement

a. Data Collection

(1) During the field ~~survey~~assessment phase, data ~~are~~is collected through observation of activities, ~~-~~document collection, and personnel interviews. Data may also be acquired through concurrent ongoing empirical data collection, such as SIGSEC monitoring.

(2) Team members must be alert to differences between what they have read, what they have assumed to be the situation, what they have been told in the command briefing, and what they observe and are told by personnel participating in the operation. Conflicting data are to be expected.

(3) While observations can verify the occurrence, sequence, and exact timing of events, much essential information must be gathered from interviews.

(a) Functional outlines should be reviewed before and after interviews to ensure that all pertinent points are covered. Specifics on how, when, and where people accomplish their tasks, and how these tasks relate to the planned and observed sequence of events, are recorded in order to document activities in a logical sequence.

(b) Team members should assure interviewees that all sources of information ~~will be~~are protected by a nonattribution policy.

(c) Interviews are best conducted by two team members.

(d) Facts to be recorded during or soon after the interview normally include:

1 Identification and purpose of the interview

2 Description of the positions occupied by the persons being interviewed

3 Details of exactly what tasks the individuals perform and how, when, and where they perform them with a view toward determining what information they receive, handle, or generate, and what they do with it

4 Whether the individuals' actions reflect an awareness of a hostile intelligence collection threat.

b. **Functional Outline Refinement**

(1) As indicated earlier, each team member should have a basic functional outline to direct data collection efforts at the beginning of the field ~~survey~~assessment phase. The basic outline ~~will be~~is modified during this phase to reflect new information obtained by observation and interview and will ultimately become a profile of actual events.

(2) Each team member should be familiar with the outlines used by the other members of the ~~survey~~assessment team and should be alert for information that might affect them. An interview in the communications area, for example, might disclose information that would result in a change to the outline being developed for operations; or an observation in one geographic location could affect an outline being followed up in another. Also, to permit followup elsewhere, all outlines should try to reflect the information generated and the flow at each location where data ~~are~~is collected.

(3) As data ~~are~~is accumulated through observation and interviews, incorporation of such data into the basic functional outline changes the original list of projected events into a profile of actual events. The functional outline then becomes a chronological record of what actually was done, where, who did it, and how and why it was done. The outline should also reflect an assessment of the vulnerability of each event to the known or suspected hostile intelligence threat.

(4) Tentative findings will begin to emerge as data collection proceeds and information is reviewed and compared. The findings should be confirmed and fully documented as quickly as possible.

(5) If a finding is considered to have serious mission impact, it should be made known to the commander responsible for the operation in order to permit early corrective actions.

(6) Development of findings during the field ~~survey~~assessment phase ensures access to supporting data and precludes the need to reconstruct evidence after the team has left the scene. Following this procedure, the basic findings and supporting data of the final ~~survey~~assessment report ~~will be~~are well developed before the end of the field ~~survey~~assessment phase. Final development and production of the ~~survey~~assessment report can then proceed immediately upon the team's return to home station.

4. Team Employment

a. The complexity, size, and duration of the ~~surveyed~~assessed operation or activity will determine the general employment of the ~~survey~~assessment team. Tentative locations for data collection, developed during the planning phase, provide initial indications of how and where to employ the team.

b. It is rarely possible, however, to plan employment in detail before the field

~~survey~~assessment phase. A limited, short duration operation with few participating elements may permit concentrating the team in one, or a very few, locations. Larger and longer operations may require complete dispersal of the team, movement of the entire team from one location to another, or both, over a substantial period of time. The most reliable guideline for the team chief in determining how to employ the team is to reassemble it daily to assess progress, compare data, and coordinate the direction of the ~~survey~~assessment.

c. The duration of the field ~~survey~~assessment phase is established during the planning phase and depends on how rapidly data are collected. Many ~~survey~~assessments have required 30 days or more in the field. Less comprehensive ones might require a week or 10 days. The proximity of data collection locations to each other, number of such locations, transportation availability, and degree of difficulty experienced in resolving conflicting data are some of the factors affecting duration of the field ~~survey~~assessment phase.

5. OPSEC ~~Survey~~Assessment Team Exit Briefing

a. An exit briefing should be presented to the commander before the team leaves a command, regardless of previous reports or tentative findings. Like the entrance briefing, the exit briefing can be an informal discussion with the commander or a formal briefing for the commander and the staff.

b. The tentative nature of ~~survey~~assessment findings should be emphasized. Even those that appear to be firm may be altered by the final data review as the ~~survey~~assessment report is prepared. Because preparation of the written report may take some time, the exit briefing can serve as an interim basis for further consideration and possible action by the commander.

c. The distribution of the final written report should be clearly stated during the exit briefing. Normally, the report ~~will be~~is provided directly to the commander. Some commands have found it useful to forward an interim report to the ~~surveyed~~assessed commander for comments before proceeding with the final version.

Intentionally Blank

ANNEX C TO APPENDIX D

ANALYSIS AND REPORTING PHASE

During this phase, the OPSEC team correlates the data acquired by individual members with information from any empirical studies conducted in conjunction with the ~~survey~~assessment.

1. Correlation of Data

a. **Correlation of Functional Outlines.** When the separate chronology outlines for each functional area are correlated, the chronology of events for the operation or activity as a whole will emerge. ~~During the field survey or analytic phases, conflicts of data must be clarified~~.Review and compare assessment data to clarify any conflicts.

b. **Functional Outlines.** The purpose of constructing the functional outlines is to describe the time-phased unfolding of the operation or activity; to depict the manner in which separate commands, organizations, and activities interact and perform their roles in the operation or activity; and to trace the flow of information through electrical and nonelectrical communications media from its origin to its ultimate recipients. It is important that the team members present the information in a manner that facilitates analysis. The net result of the correlation will be a portrayal of the entire operation or activity.

c. **Correlation of Empirical Data.** In addition to correlating data acquired from the observations of individual team members, the ~~survey~~assessment team may also use relevant, empirically derived data to refine individual functional outlines. More importantly, these data can also verify vulnerabilities that would otherwise be exceedingly speculative or tenuous. Empirical data are extremely important to a comprehensive ~~survey~~assessment.

2. Identification of Vulnerabilities

a. The correlation and analysis of data helps the team to refine ~~the~~ previously identified preliminary vulnerabilities or isolate new ones. This analysis is accomplished in a manner similar to the way in which adversaries would process information through their intelligence systems.

b. Indicators that are potentially observable are identified as vulnerabilities. Vulnerabilities point out situations that an adversary may be able to exploit. The key factors of a vulnerability are observable indicators and an intelligence collection threat to those indicators.

c. The degree of risk to the friendly mission depends on the adversary’s ability to react to the situation in sufficient time to degrade friendly mission or task effectiveness.

3. OPSEC Assessment Report

a. The report of the OPSEC ~~survey~~assessment is addressed to the commander of the ~~survey~~assessed operation or activity. Lengthy reports (more than 15 pages) should be accompanied by an executive summary.

b. There is no special format for OPSEC ~~survey~~assessment reports; a suggested format is found in Tab A, “Suggested Format for Final OPSEC ~~Survey~~Assessment Format.” Whatever the format, the report should provide a discussion of identified critical information, indicators, adversaries and their intelligence capabilities, OPSEC vulnerabilities, risk analysis, and recommended OPSEC measures to eliminate or reduce the vulnerabilities. Although some vulnerabilities may be virtually impossible to eliminate or reduce, they ~~should be~~are included in the report to enable commanders to assess their operation or activity more realistically.

c. Each report should contain a threat statement. Its length and classification need only be adequate to substantiate the vulnerabilities (or actual sources of adversary information) described in the report. The statement may be included in the main body of the report or as an annex~~ to it~~. Portions of the threat that apply to a particular vulnerability finding ~~may be~~is concisely stated as substantiation in a paragraph preceding or following the explanation of the observation. If the threat statement is so classified that it will impede the desired distribution and handling, the statement, or parts of it, should be affixed as an annex that ~~can be~~is included only in copies of the

~~survey~~assessment report provided to appropriately cleared recipients.

d. The section that delineates vulnerabilities can be presented in a sequence that correlates with their significance, in an order that coincides with their appearance in the chronological unfolding of the ~~survey~~assessmented operation or activity, or grouped together according to functional area (logistics, communications, personnel). A particular vulnerability can be introduced by a headline followed by an adequate description of the finding and accompanied by identification of that portion of the operation or activity that includes the vulnerability. As stated earlier, a vulnerability observation may also include relevant threat references.

e. If possible, OPSEC teams should include recommendations for corrective actions in the report. However, the team is not compelled to accompany each vulnerability finding with a recommendation. In some situations, the team may not be qualified to devise the corrective action; in others, it may not have an appreciation of the limitations in resources and options of a particular command. It may sometimes be more effective for the team to present the recommendation informally rather than including it in the ~~survey~~assessment report. Recommendations of the OPSEC team may be particularly valuable in situations in which a vulnerability crosses command lines. Ultimately, commanders or the responsible officials must assess the effect of possible adversary exploitation of vulnerabilities on the effectiveness of their operation or activity. They must then decide between implementing corrective actions or accepting the risk posed by the vulnerability.

f. Appendixes and annexes to OPSEC ~~survey~~assessment reports may be added to support the vulnerability findings and conclusions. Sections, such as a threat annex, may include empirical studies (or parts of them). Maps, diagrams, and other illustrative materials are some ways to substantiate OPSEC vulnerabilities.

g. The report may end with a conclusion or summary of the ~~survey~~assessment and its findings. The summary should not include judgments about compliance with standing security practices of the organizations. Such judgments are the purview of security disciplines.

h. Distribution of the ~~survey~~assessment team's report should be limited to the principal commands responsible for the ~~survey~~assessmented operation or activity. After the commands have had time to assess the report and take corrective actions, they can consider additional distribution. Abstracts from the report may be provided for lessons-learned documents or data bases on a nonattribution basis.

i. Because they contain vulnerability information, OPSEC ~~survey~~assessment reports must be controlled from release to unauthorized persons or agencies. Affected portions of the report ~~must be~~are controlled in accordance with applicable security classification guides. For those portions of the report not controlled by security classification guides, administrative control of the release of ~~survey~~assessment report information must be considered. Likewise, the notes, interviews, and raw data used to build a

~~survey~~assessment report ~~must be~~are subject to the same controls as the finished report.

TAB A TO ANNEX C TO APPENDIX D

SUGGESTED FORMAT FOR FINAL OPSEC ~~SURVEY~~ASSESSMENT REPORT

1. Overview

____a. Background. Address the purpose and scope of the ~~survey~~assessment as well as the results of the threat and vulnerability assessments.

____b. Conduct of ~~Survey~~Assessment. Brief discussion of methodology, team composition, major commands visited, and timeframe of ~~survey~~assessment.

____c. Critical Information

____d. Threat

2. Summary of Significant Findings

3. Analysis, Conclusions, and Findings

____This is the body of the report. Discussions and findings may be listed chronologically, by command, or chronologically within commands.

4. The Suggested Format for Each Finding

a. Observation

b. Analysis and discussion

c. Conclusion or recommendation

APPENDIX E

REFERENCES

The development of Joint Pub 3-54 is based on the following primary references:

1. DOD Directive 5205.2, *DOD Operations Security Program*.

2. CJCSI 3210.03, *Joint Electronic Warfare Policy.*

3. CJCSI 3211.01C, *Joint Policy for Military Deception*.

4. CJCSI 3213.01A, *Joint Operations Security*.

5. CJCSM 3122.01, *Joint Operation Planning and Execution System, Vol I: (Planning Policies and Procedures).*

6. CJCSM 3122.03A, *Joint Operation Planning and Execution System, Vol II: (Planning and Execution Formats and Guidance)*.

7. Joint Pub 1, *Joint Warfare of the Armed Forces of the United States*.

8. Joint Pub 1-02, *Department of Defense Dictionary of Military and Terms*.

9. Joint Pub 2-0, *Doctrine for Intelligence Support to Joint Operations.*

10. Joint Pub 3-0, *Doctrine for Joint Operations*.

11. Joint Pub 3-13, *Joint Doctrine for Information Operations*.

12. Joint Pub 3-51, *Joint Doctrine for Electronic Warfare.*

13. Joint Pub 3-53, *Doctrine for Joint Psychological Operations.*

14. Joint Pub 3-58, *Joint Doctrine for Military Deception*.

15. Joint Pub 3-61, *Joint Doctrine fro Public Affairs Operations.*

~~TAB A TO ANNEX A TO APPENDIX E~~

~~COMPOSITE OPSEC PROFILE FOR COMBAT OPERATIONS~~

~~Figure E-A-A-1 provides a sample composite OPSEC profile for combat operations. As illustrated by this sample, a profile can be constructed to display the event-time-agency data of significant information collected during an OPSEC survey. OPSEC survey personnel should use a composite OPSEC profile or similar tool to assist in identifying unit or mission OPSEC indicators.~~

COMPOSITE OPSEC PROFILE: BRIGADE COMBAT ASSAULT

(HOURS)	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	H
ADMIN													17		11										
INTELL									3 4						12 13										
OPS																	15	16						24	
LOG							2						8	9 10											
COMMS						1				5 6 7					14				18	19	20	21	22	23	

1.	1100:	Warning order over unsecure telephone at TF HQ.
2.	1233:	AF supply order 1500 x 500 lb bombs.
3.	1310:	S2 order for 100 x 1:12,500 maps of objective area.
4.	1320:	Recon flight over forest clearings in objective area.
5.	1405:	Artillery net activated; warning to move tubes.
6.	1406:	Brigade maintenance net unusually active.
7.	1430:	Dustoff net disclosed establishment of field aid station.
8.	1705:	12 x sling-loaded CH-47s arrived at Brigade rear.
9.	1800:	3 x C-123s off-loading wooden crates (probably artillery rounds).
10.	1850:	5 x C-123s off-loading fuel doughnuts.
11.	1930:	Two troops of 1-9th Air Cav released to rear on personal business "in time to return for the operation."
12.	1940:	Sniffer flight in objective area.
13.	1944:	ARDF flight observed in objective area.
14.	1921:	LRRP radio DF'd in objective area.
15.	2100:	Pathfinders assemble outside Brigade briefing tent.
16.	2230:	Artillery firing H&I in objective area for first time.
17.	2315:	Chaplain holding services near forward positions.
18.	2340:	New frequency/cell sign heard.
19.	0030:	New NCS policies chatters for first time.
20.	0130:	More new frequencies/call signs; many comms checks.
21.	0230:	Only active stations in Brigade rear.
22.	0330:	Near complete radio silence.
23.	0430:	Complete radio silence.
24.	0455:	Many flares.

~~**Intentionally Blank**~~

APPENDIX F

ADMINISTRATIVE INSTRUCTIONS

1. User Comments

____Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command Joint Warfighting Center Code JW100, 116 Lake View Parkway, Suffolk, VA 23435-2697 These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

____The lead agent and the Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

3. Supersession

____This publication supersedes JP 3-54, 24 January 1997, *Joint Doctrine for Operations Security*.~~, with Change 1.~~

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J-3/DDIO//
INFO: JOINT STAFF WASHINGTON DC//J7-JDETD//
USCINCJFCOM SUFFOLK VA//JW100//

Routine changes should be submitted to the Director for Operational Plans and Joint Force Development (J-7), JDETD, 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000, with info copies to the USJFCOM JWFC.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE	COPY	DATE OF	DATE	POSTED	
NUMBER	NUMBER	CHANGE	ENTERED	BY	REMARKS

____

____

____

5. Distribution

____a. Additional copies of this publication can be obtained through Service publication centers listed below (initial contact) or the USJFCOM JWFC in the event that the joint publication is not available from the Service.

____b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PSS, PO-FL, Room 1A674, Pentagon, Washington, D.C. 20301-7400.

____c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "*Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands*."

________Army: ____US Army AG Publication Center SL
________ ________1655 Woodson Road

Attn: Joint Publications
St. Louis, MO 63114-6181

Air Force: Air Force Publications Distribution Center
2800 Eastern Boulevard
Baltimore, MD 21220-2896

Navy: CO, Naval Inventory Control Point
700 Robbins Avenue
Bldg 1, Customer Service
Philadelphia, PA 19111-5099

Marine Corps: Commander (Attn: Publications)
814 Radford Blvd, Suite 20321
Albany, GA 31704-0321

Coast Guard: Commandant Coast Guard (G-OPD), US Coast Guard
2100 2nd Street, SW
Washington, D.C. 20593-0001

Commander
USJFCOM JWFC Code JW2102
Doctrine Division (Publication Distribution)

116 Lake View Parkway
Suffolk, VA 23435-2697

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R, *Information Security Program*.

Intentionally Blank

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

AOR	area of responsibility
C2	command and control
C4I	command, control, communications, computers, and intelligence
CA	civil affairs
CJCS	Chairman of the Joint Chiefs of Staff
CNA	computer network attack
COA	course of action
COMSEC	communications security
CONPLAN	operation plan in concept format
DIA	Defense Intelligence Agency
DDIO	Deputy Director of Information Operations
DOD	Department of Defense
DTRA	Defense Threat Reduction Agency
~~EEFI~~	~~essential elements of friendly information~~
EW	electronic warfare
IO	information operation
~~IW~~	~~information warfare~~

JCMA	Joint (communications security) COMSEC Monitoring Activity
JFC	joint force commander
JOPES	Joint Operation Planning and Execution System
JPG	joint planning group
LEA	law enforcement agency
~~MASINT~~	~~measurement and signature intelligence~~
~~MOOTW~~	~~military operations other than war~~
OEG	OPSEC Executive Groups
OPLAN	operation plan in complete format
OPORD	operation order
OPSEC	operations security
PAO	public affairs officer
PSYOP	psychological operations
SIGINT	signals intelligence
SIGSEC	signal~~s~~ security
SIO	special information operations

SOP	standard operating procedure
WAN	wide-area network

PART II—TERMS AND DEFINITIONS

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called **C2.** (JP 1-02)

~~**command and control warfare.** The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is a warfighting application of information warfare in military operations and is a subset of information warfare. Command and control warfare applies across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade or destroy the friendly C2 system. (JP 1-02)~~

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC.** (JP 1-02)

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. (JP 1-02)

critical information. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. See also **counterdeception; military deception.** (JP 1-02)

~~**essential elements of friendly information**. Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. Also called EEFI. (Joint Pub 1-02)~~

defensive information operations. The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (JP 1-02)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO.** (JP-3-13)

information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called **IW**. See also crisis; information; information operations; operation. (JP 1-02)

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives. These capabilities and activities include but are not limited to operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could also include computer network attack (JP1-02)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: 1. Identify those actions that can be observed by adversary intelligence systems. 2. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. 3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 1-02)

operations security indicators. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (JP 1-02)

operations security measures. Methods and means to gain and maintain essential secrecy about critical information. The following categories apply: 1. action control. The objective is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake; decide whether or not to execute actions; and determine the “who,” “when,” “where,” and “how” for actions necessary to accomplish tasks. 2. countermeasures. The objective is to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering and processing capabilities. 3. counteranalysis. The objective is to prevent accurate interpretations of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers. (JP 1-02)

operations security planning guidance. Guidance that serves as the blueprint for operations security planning by all functional elements throughout the organization. It defines the critical information that requires protection from adversary appreciations, taking into account friendly and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations, and pertinent intelligence system threats. It also should outline provisional operations security measures to ensure the requisite essential secrecy. (JP 1-02)

operations security vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making. (JP 1-02)

signal security. A generic term that includes both communications security and electronic security. (JP1-02)

special information operations. Information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. Also called SIO. (JP1-02)

Intentionally Blank

JOINT
CHIEFS OF STAFF