



U.S. Army War College
Dept. of Military Strategy, Planning, and Operations
&
Center for Strategic Leadership

December 2007
AY08 Edition

U.S. Army War College

Information Operations Primer

Fundamentals of Information Operations

Middle States Accreditation

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



DEPARTMENT OF THE ARMY
UNITED STATES ARMY WAR COLLEGE AND CARLISLE BARRACKS
CARLISLE, PENNSYLVANIA 17013-5217

REPLY TO
ATTENTION OF

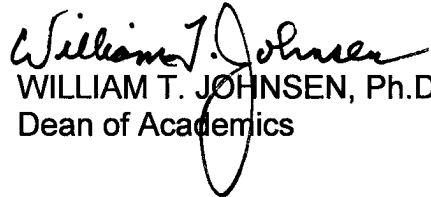
ATWC-A

21 December 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army War College Information Operations Primer

This is a document prepared primarily for use by the staff, faculty, and students of the U.S. Army War College. It is not intended for general distribution. DoD entities may reprint this document or portions of it without further permission from the U.S. Army War College. Non-DoD individual or organization requests to reprint will be handled on a case-by-case basis.


WILLIAM T. JOHNSEN, Ph.D.
Dean of Academics

DISTRIBUTION:
DMSPO 500

This Page Intentionally Blank

Forward

This document provides an overview of Department of Defense (DoD) Information Operations (IO) doctrine and organizations at the joint and individual service levels. It is intended to serve students and staff of the US Army War College as a ready reference for IO information extracted and summarized from a variety of sources. Wherever possible, Internet web sites have been given to provide access to additional and more up-to-date information. The booklet is intentionally UNCLASSIFIED so that the material can be easily referenced during course work, while engaged in exercises, and later in subsequent assignments.

This booklet begins with an overview of Information Operations and Strategic Communication. The booklet then goes from the national level to the Department of Defense, to the Joint Operations level and then finally to the service level. At each level it describes strategies or doctrine, agencies, organizations, and educational institutions dedicated to the information element of national power. Finally, the document concludes with an overview of Information Operations Condition (INFOCON) and an IO specific glossary.

Readers will note that many of the concepts, documents, and organizations are “works in progress” as DoD and the services strive to address the challenges of a rapidly changing IO environment. Thus, this summarization effort is on-going and continuous. Please address any suggested additions, revisions and/or corrections to the primary points of contact below for inclusion in subsequent editions.

Special thanks and recognition is given to the following individuals throughout the Department of Defense whose help and assistance have made this revision of the Primer possible: Ambassador Brian E. Carlson, Office of the Under Secretary of State Public Diplomacy and Public Affairs, Ms. Chris Adams, and Ms. Kelly Layman (both of the Joint Warfare Analysis Center); COL Steve Campbell, USA (JPASE); Mr. Roberto Rodriguez (Joint Staff, J-39,DDGO); Maj David Clapp, USMC, (Marine Corps Combat Development Command); MAJ Justin Hickman, USA and Mr. Anthony Maybrier (JIOWC); Maj Steven Dennis, USAF (Air Force Information Operations Center); Mr. Philip Marotto, (OUSD-Policy); Maj Margie L. Gabriel, USAF (Air Force Intelligence Surveillance and Reconnaissance Agency); LTC Brian Russo, USA (OUSD-Intelligence); Capt Stephanie Helm, USN (Naval War College); Mr. Max Willey (Navy IO Command Norfolk), MAJ Joel P. Humphries, USA (USSTRATCOM); COL Wayne Dudding, USA and LTC Meg Roosma, USA (ARIOC), Mr. Steve Iatrou (Naval Postgraduate School); COL Greg Julian, USA (OSD- Public Affairs); Mr. Tom Lopez and CAPT. Key Watkins, USN (both of OASD-NII); COL Steve Mayhew, USA, and Mr. Jerry Luss (both of JTF-GNO); Mr. William D. Malone, (Naval Information Operations Command-Norfolk); Col Robert Morris, USAF and Mr. Brian Gouker (both of NSA); CDR Ray Moses, USN and LTC Samuel Caccamo, USA (Joint Forces Staff College); Maj Charles Sammons USAF (8th AF); Ms. Tara Shea, (Information Assurance Technology Analysis Center); Mr. Eric C. Vernon and Mr. Steven Shires (both of 1st Information Operations Command); Col James E. Smith, USAF (Air War College); COL Jack Summe, USA and COL Carl Phillips, USA (both of JPSE); Mr. Paul Tiberi and LTC Timothy Washington, USA (Army Combined Arms Center); Maj Nichole Oliver USAF (AETC AFDDEC/DDS), Maj Alberto Samonte, USAF (Air Force Doctrine Center); Ms. Elissa Bendel and CDR Jeff Lamont (USN) (both of DISA, DSO), Ms. Lillie Cofield, (DISA), LCDR Marc Boyd, USN (USSOCOM) and Mr. Jerry Johnson (CSL-IWG).

Portions of this document may be quoted or reprinted without further permission, with credit to the original source document/web site or the US Army War College, as appropriate. Posting as a complete PDF file to US government web-sites must be done with authorization of the U.S. Army War College, Carlisle Barracks, PA. Please address all such requests to: COL David Smith or Professor Dennis Murphy – see next page for addresses.

COL David J. Smith
Department of Military Strategy,
Planning, and Operations
U.S. Army War College
122 Forbes Avenue, Rm C-102
Carlisle Barracks, PA 17013-5242
717-245-3455
davidj.smith@us.army.mil

Professor Dennis M. Murphy
Professor of Information Operations/Information
in Warfare
U.S. Army War College, Center for Strategic
Leadership
650 Wright Avenue
Carlisle, PA 17013
717-245-3937
Dennis.Murphy@us.army.mil

Summary of Changes to the AY07 Edition

The following changes have been made in this edition of the IO Primer:

Re-organization of the Primer

After the Introduction to Information Operations and the section on Strategic Communication, the document has been re-organized to flow from the national level the DoD, to the Joint Level, and then finally to the service level. At each level, there are descriptions of strategy or doctrine and then agencies or organizations dedicated to the information element of national power.

Additions:

- Description of the U.S. National Strategy for Public Diplomacy and Strategic Communication.
- Synopsis of the QDR Execution Roadmap for Strategic Communication.
- Description of the Army Reserve Information Operations Command.

Revisions:

- The “Information Operations” (previously “Introduction”) and “Strategic Communication” sections have been updated.
- DoD offices and agency sections have been updated where appropriate.
- The Marine Corps section has been updated, while the Army, Navy, and Air Force portion remain the same. Both the Army and Air Force are currently reviewing doctrine but no significant changes at the time of printing of the Primer.
- Every section has been reviewed by the responsible office and most sections have some changes.
- The Air Intelligence Agency was re-designated as the Air Force Intelligence, Surveillance and Reconnaissance Agency on 8 June 2007.

This Page Intentionally Blank

TABLE OF CONTENTS

Forward	iii
Summary of Changes to the AY07 Edition	v
Table of Contents	vii
Information Operations.....	1
Strategic Communication.....	9
National Strategy and Agencies.....	15
U.S. National Strategy for Public Diplomacy and Strategic Communication.....	15
National Security Agency (NSA).....	17
Department of Defense Directives and Roadmaps	21
Department of Defense Directive (DoDD) O-3600.01 Information Operations	21
The Information Operations (IO) Roadmap, 2003	25
QDR Execution Roadmap for Strategic Communication.....	29
Department of Defense Organizations.....	31
Under Secretary Of Defense – Policy (USD(P))	33
Under Secretary Of Defense for Intelligence (USD(I)).....	37
Assistant Secretary Of Defense – Networks And Information Integration (ASD(NII))	39
DoD Strategic Communication Integration Group (SCIG)	41
Defense Information Systems Agency (DISA)	45
Information Assurance Technology Analysis Center (IATAC)	49
Joint Information Operations Doctrine and Vision.....	51
Joint Information Operations Doctrine.....	53
Joint Vision 2020 and Information Superiority	61
Joint Organizations and Educational Institutions	63
Joint Staff, Deputy Director for Global Operations (DDGO)	65
Joint Spectrum Center (JSC)	67
Joint Warfare Analysis Center (JWAC)	71

U. S. Strategic Command (USSTRATCOM).....	73
U. S. Special Operations Command (USSOCOM)	83
Joint Forces Staff College Information Operations Program	91
Information Operations Center of Excellence, Naval Postgraduate School.....	93
Service Information Operations Doctrine.....	95
Army Information Operations Doctrine	97
Marine Corps Information Operations Doctrine	109
Navy Information Operations Doctrine.....	115
Air Force Information Operations Doctrine	123
Service Component Information Operations Organizations.....	133
Army – 1st Information Operations Command (1st IO Cmd)	135
Army - Army Reserve Information Operations Command (ARIOC).....	137
United States Army Information Operations Proponent (USAIOP)	139
Navy - U.S. Navy Information Operations Organizations	141
Air Force Intelligence, Surveillance and Reconnaissance Agency	143
Air Force Information Operations Center (AFIOC)	145
Air Force - Eighth Air Force	149
Information Operations Conditions (INFOCONs).....	151
Glossary	161

Information Operations



Few topics seem to have as much controversy or discussion as, “What are Information Operations (IO)?” The emergence of the term Strategic Communication (SC) has added to the potential confusion as both are applications of the information element of national power. This introduction and the following essay attempt to answer that question by examining both IO and SC conceptually and doctrinally. They are intended as a guide to these topics to facilitate academic discussion and are not authoritative. Throughout this discussion, various terms may be defined less formally to facilitate understanding and comprehension. The reader is directed to Joint Publication 1-02, as required, for the approved formal definitions.

Information Operations are an evolving construct with historical roots back to antiquity. Thus it is both an old and a new concept. The late 1970’s saw the emergence of Information Warfare (IW) and Command and Control Warfare (C2W) as war-fighting constructs integrating several diverse capabilities. IW and C2W, in turn, evolved into Information Operations recognizing the critical role of information as an element of national power through the full spectrum of peace, conflict, and war.

So what are Information Operations?

1. IO as an Integrating Function. Information Operations are essentially the *integration of specified capabilities involving information and information systems.* This concept is similar to Joint Operations which are the integration of service capabilities or Combined Operations which are the integration of two or more forces or agencies of two or more allies. The integration envisioned is not mere deconfliction, but the synchronization and harmonization of activities whose resulting effect is significantly greater than the sum of the individual components. While this writes well and briefs well, it is the foundation for successful employment of IO.

IO are normally performed by military forces at both the operational and tactical levels. IO at the strategic level are a critical component of strategic communication.

Several questions logically follow:

- a. What capabilities are integrated?
- b. How are they integrated?
- c. Towards what end?

Following the concept of “begin with the end in mind,” the last question will be considered first.

2. Purpose of IO. Information Operations seek to influence the *behavior* of target decision-makers or audiences through the use of information and information systems. Conversely, Information Operations also seek to shield or defend friendly decision-makers or audiences from being unduly influenced by a target’s use of information or information systems. This is no different from the exercise of the other forms of national power, be they diplomatic, military, or economic. In this instance the means is information, but the resulting outcome is the same.

a. This use of information is frequently referred to as “soft-power” or “non-kinetic” as contrasted with the military use of kinetic (both lethal and nonlethal) means to physically attack a target.

b. However, IO also encompass activities to disrupt, degrade, or destroy adversary information systems. This includes physical destruction. Isolating an enemy decision-maker by eliminating his ability to command and control his forces is certainly a means of influencing his behavior.

c. One of the primary focuses of IO is the “adversary decision-makers” or “adversary decision-making processes.” Efforts to influence a wider range of potential audiences are often more appropriately termed Strategic Communication. The use of IO to influence domestic audiences is strictly prohibited by law to prevent abuse of that capability.

d. Affecting the target’s decision cycle (sometimes referred to as his “OODA-loop” (observe, orient, decide, act - loop)) is a means of influencing target behavior. Obviously, reducing an adversary’s ability to make timely and effective decisions will degrade his exercise of initiative or his response to friendly military action.

e. Action must also be taken to shield or protect friendly information and information systems from compromise or disruption. As a network-enabled force, the United States is particularly reliant on these systems to maintain situational awareness and to command and control friendly forces.

f. These protective actions are not intended to prevent the unrestricted flow of information vital to a free society. They are intended to prevent a target’s manipulation or distortion of information or attacks on information systems from being effective.

3. **An IO Conceptual Model.** At this point, a model would be helpful to conceptualize the kind of activities which would be effective in achieving the desired result (influence target behavior, protect friendly behavior from being influenced).

a. All Information Operations activities occur within the broader context of an *information environment*. This environment recognizes the critical role that information and information systems play in today’s advanced societies as they progressed along a continuum from agrarian, to industrial, to the information age. This environment pervades and transcends the boundaries of land, sea, air, space, and cyberspace.

b. Within this environment exist three conceptual dimensions: physical, information, and cognitive as depicted in Figure 1, representing a target’s decision cycle.

(1) The physical dimension is the tangible real world. It is the dimension where military operations take place within the land, sea, air, space, and cyberspace environments. Information and communications systems (infra-structure) exist within this dimension to enable these operations to take place.

(2) The information dimension is where information is created, manipulated, shared, and stored. This dimension links the physical real world with the human consciousness of the cognitive dimension both as a source of input (stimulus, senses, etc.) and to convey output (intent, direction, decisions, etc.). These linkages are shown as arrows in the figure.

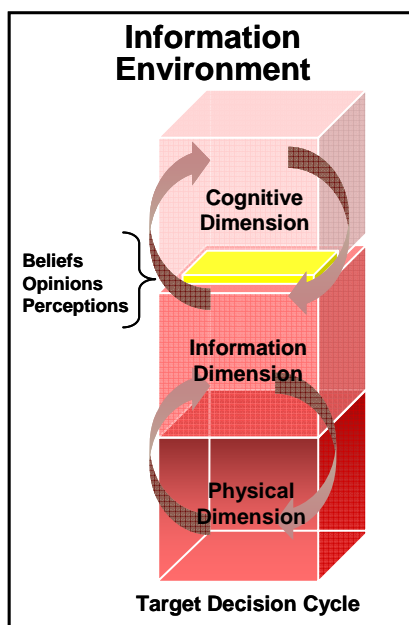


Figure 1. Information Environment

(3) The cognitive dimension exists in the mind. This is where the individual processes the received information according to a unique set of perceptions (interprets the information), opinions (within a greater context of how he sees the world organized), and beliefs (on a foundation of core central values). These attributes act as a “window” to filter the information and provide a sense of meaning and context. The information is evaluated and processed (via an O-O-D-A loop or other model) to form decisions which are communicated back through the information dimension to the physical world. It should be noted that the cognitive dimension can not be directly attacked (short of mind-altering drugs, etc.) but must be influenced indirectly through the physical and information dimensions.

(4) Not shown in the figure is an additional “social” dimension which links the individual to others forming a greater social network. This social network plays a critical role in the human decision-making process as well.

c. In a similar manner, the friendly decision cycle can be represented in relationship to the target as shown in Figure 2. This allows several terms to be defined conceptually.

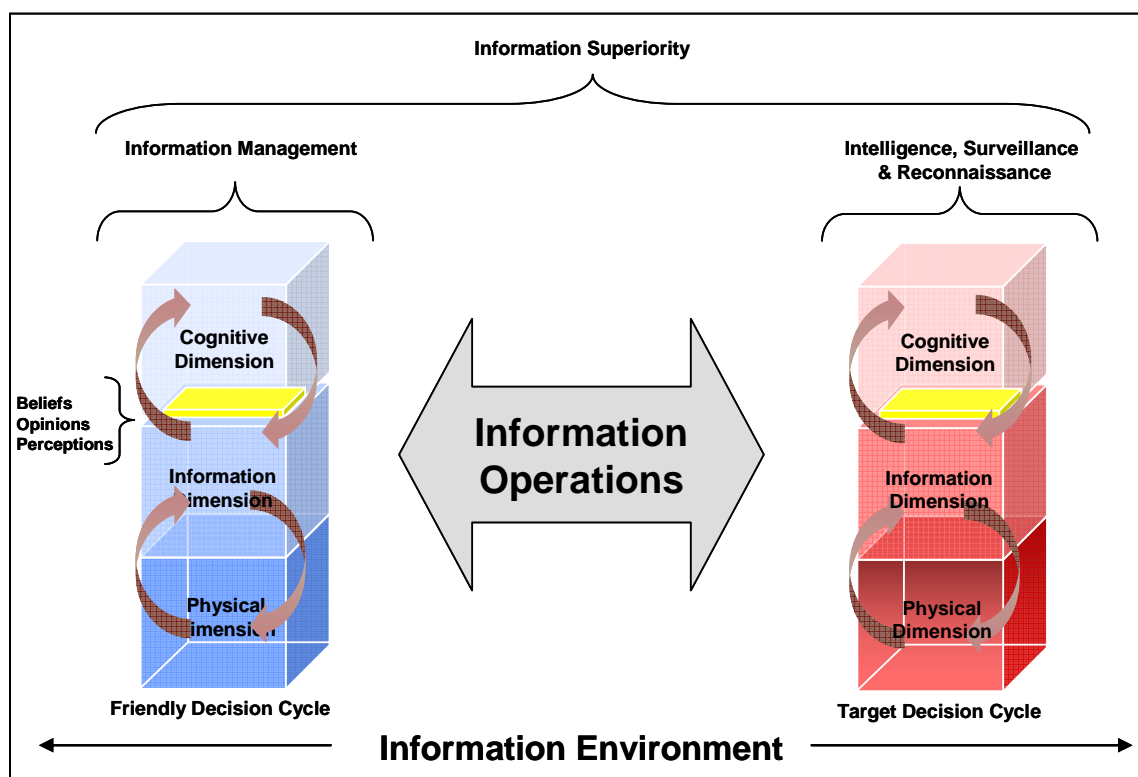


Figure 2. A Notional Information Operations Model

(1) **Intelligence, Surveillance, and Reconnaissance (ISR)** are those activities which synchronize and integrate the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems to gain information and knowledge concerning a target (adversary). The focus is strictly on target information and information systems.

(2) Correspondingly, **Information Management (IM)** activities seek to provide the right information to the right individual at the right time in a usable form to facilitate situational understanding and decision-making. The focus is on friendly information and information systems.

(3) The third type of activity relates to both friendly and target decision cycles. These activities are **Information Operations (IO)** as indicated in Figure 2.

(4) Considering these three sets of activities as a whole yields **Information Superiority** which, when achieved, results in a degree of dominance in the information domain (environment) permitting the conduct of operations without effective opposition. Information Superiority is a key enabler of Joint Vision 2020 and Network-centric Operations.

d. Information Operations can now be depicted as attempting to influence, disrupt, corrupt, or usurp adversarial human or automated decision-making while protecting friendly decision-making as shown in Figure 3.

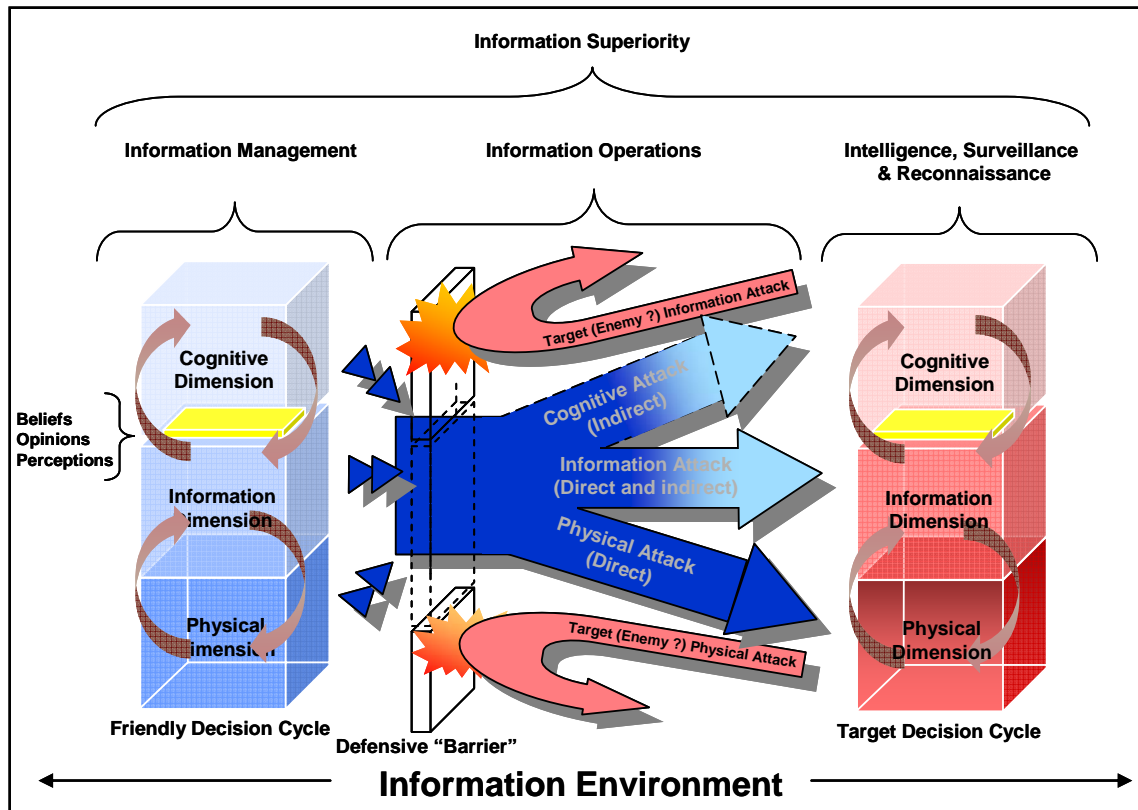


Figure 3. Information Operations Conceptual Framework

4. IO Capabilities. Using this framework, it is now possible to address the question of what capabilities are integrated by IO. These capabilities will be further categorized as either core, supporting, or related.

a. **Core Capabilities** are those which are essential to the conduct of IO by providing critical operational effects or preventing the adversary from doing so. The five core capabilities of Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC), Electronic Warfare (EW), and Computer Network Operations (CNO) form the foundation for IO. While not every activity conducted within these capabilities is IO, they all contribute to the achievement of IO objectives.

(1) **Psychological Operations (PSYOP)** are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

(2) **Military Deception (MILDEC)** consists of actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby

causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

(3) **Operations Security (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 indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and
- (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

(4) **Electronic Warfare (EW)** is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are as follows:

(a) Electronic Attack (EA). That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

(b) Electronic Protection (EP). That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

(c) Electronic Warfare Support (ES). That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence.

(5) **Computer Network Operations (CNO)**. Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

(a) Computer Network Attack (CNA). Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

(b) Computer Network Defense (CND). Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.

(c) Computer Network Exploitation (CNE). Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

b. These five core capabilities are supported by five additional, or **Supporting Capabilities** which provide additional, though less critical, operational effects: Information Assurance (IA), Physical Security, Physical Attack, Counterintelligence (CI), and Combat Camera (COMCAM).

(1) **Information Assurance (IA)** is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

(2) **Physical Security** is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. The physical security process includes determining vulnerabilities to known threats, applying appropriate deterrent, control, and denial safeguard techniques and measures, and responding to changing conditions.

(3) **Physical Attack** disrupts, damages, or destroys adversary targets through destructive power. Physical attack can also be used to create or alter adversary perceptions or drive an adversary to use certain exploitable information systems.

(4) **Counterintelligence (CI)** consists of the information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassination conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

(5) **Combat Camera (COMCAM)** consists of the acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services.

c. Finally, three additional **Related Capabilities** of Public Affairs (PA), Civil-Military Operations (CMO), and Defense Support to Public Diplomacy (DSPD) contribute to the accomplishment of the IO mission. These activities often have regulatory, statutory, or policy restrictions and limitations regarding their employment which must be observed.

(1) **Public Affairs (PA)** are those public information, command information, and community relations activities directed towards both the external and internal publics with interest in the Department of Defense.

(2) **Civil-Military Operations (CMO)** are the activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces.

(3) **Defense Support to Public Diplomacy (DSPD)** are those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government (previously referred to as Military Support to Public Diplomacy).

d. These capabilities can be summarized as shown in the following table.

<u>CORE CAPABILITIES</u>	
Electronic Warfare	Military Deception
Computer Network Operations	Psychological Operations
Operations Security	
<u>SUPPORTING CAPABILITIES</u>	<u>RELATED CAPABILITIES</u>
Information Assurance	Public Affairs
Physical Security	Civil-Military Operations
Counterintelligence	Defense Support to Public Diplomacy
Physical Attack	
Combat Camera	
<u>DoD Information Operations:</u> “The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own.”	

Table 1. Joint IO Definition

e. These activities can be related to the IO Conceptual Framework previously described in terms of offensive and defensive actions as well as in terms of their orientation with respect to the cognitive, information, and physical dimensions. An additional distinction which may be helpful is to further categorize the activities into those which are primarily “influential” in nature (MILDEP, PSYOP, PA, etc.) and those which are more “technical (or electronic)” in nature (EW and CNO, etc.).

5. **IO Planning and Execution.** Having identified the purpose of IO and the activities associated with it, the third question will now be addressed concerning how IO capabilities are integrated.

a. Information Operations are planned by the IO section of a joint or service staff under the direction and supervision of a designed IO officer or cell chief. Normally this section resides within the operations division (J-3) of the staff. Current Army IO doctrine directs the creation of a separate primary staff section (G-7) responsible for IO planning and execution.

b. To further integrate and synchronize IO activities, an “IO Cell” is established under the leadership of the IO cell chief. Representatives from the core, supporting, and related capabilities as well as the special staff, service/functional components, and appropriate national agencies serve as members.

c. IO planning should be fully integrated into the overall joint planning process, be it contingency or crisis action. There should not be a separate “IO campaign plan” just as there is not a separate “maneuver campaign plan.”

d. Products from the IO planning process are incorporated into the Commander’s Estimate, Commander’s Concept, and the OPLAN/OPORD as documented in the Joint Operation Planning and Execution System (JOPES).

e. Additionally, IO planners and operators should be represented within the Effects and Effects Coordination Cell where operational fires (both kinetic and non-kinetic) are integrated and synchronized.

f. Execution of the IO portion of the joint plan is done by both dedicated IO forces (PSYOP, EW, CNO, etc.) and general purpose forces tasked for that purpose (MILDEP, OPSEC, etc.).

g. Evaluation of the success of the execution of the plan is done through identified measures of effectiveness (how well the plan achieved the desired result) as well as through measures of performance (how well the plan was executed).

6. **Additional Considerations.**

a. Long term success in any interpersonal endeavor (of which military operations are a part) is a function of influencing the perceptions, opinions, beliefs, and ultimately the behavior of a target audience. This influence can range from compellence and coercion on one end of the spectrum to cooperation and collaboration on the other. It must be recognized that everything that is done and said as well as the visual impression that is created (actions, words, and images) contribute to either altering or reinforcing the target's perceptions, opinions, and beliefs – with words making perhaps the least significant contribution.

b. The ability to influence a target audience is a function of the relationship that exists between the two parties and the corresponding trust level. One of the first tasks for the conduct of effective IO is to build relationships and establish credible messages from credible messengers using credible media. Without credibility, there is little or no chance the target's perceptions, opinions, and beliefs will be positively effected.

c. Even when done effectively, IO effects typically take longer to achieve and are more difficult to measure than conventional operations. Therefore, a long term commitment to building relationships and maintaining communication (two-way dialog) is critical. Theater Security Cooperation Plans are a vital part of this effort. Waiting until a crisis occurs and then “throwing info ops at it” is an exercise in futility.

d. An appropriate understanding of the target's culture and norms is essential. The tendency to “mirror” friendly cultural values and perspectives must be avoided. The preparation of IO products and an evaluation of their potential effectiveness must be done from the perspective of the recipient (target audience) through their cultural lens. This is especially true during the “product review and approval” process when what may appear to be an unsophisticated and even amateurish looking product (leaflet, flyer, handbill, etc.) may, in fact, be exactly the proper vehicle for conveying the desired message.

e. Therefore, effectively wielding the information element of national power is fundamentally an application of these concepts to achieve the desired effects in the information environment.

Effective IO leverages the power of information to complement the other instruments of national power resulting in the achievement of national objectives with less expenditure of blood and treasure.

COL David J. Smith
Department of Military Strategy, Planning, and Operations
U.S. Army War College

Updated: November 2007.

Strategic Communication



Strategic Communication. This section addresses some considerations of the information element of power at the strategic level.

a. Information and National Power. Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.¹ Subsequent national security documents allude to different aspects of information but without a specific strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power...and that information is woven through the other elements since their activities will have an informational impact.² Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: “use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security.”³ Information as power is wielded in an increasingly complex environment consisting of the physical, information, and cognitive dimensions as previously defined.

b. Strategic Communication Overview. The executive branch of the US government has the responsibility to develop and sustain an information strategy that ensures that themes and messages are promulgated consistent with policy. This strategy should guide and direct communications activities across the information environment. Effective Strategic Communication is the desired “way” (given the “ends, ways, means” model) that information is wielded in accordance with that strategy. **Strategic Communication** can be described as the proactive and continuous process that supports the national security strategy by identifying and responding to strategic threats and opportunities with information related activities. It is “focused United States Government processes and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power” whose primary supporting capabilities are Public Affairs; military Information Operations (IO) and Public Diplomacy.⁴ These capabilities are described below:

(1) Public affairs and military IO have been defined in the context of their use within the Department of Defense (DOD) in the previous section.

(2) Public diplomacy is primarily practiced by the Department of State (DOS). It is defined as “those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad.”⁵

(3) International broadcasting services are cited as a strategic communication means in some definitions. Under the supervision of the Broadcasting Board of Governors (BBG), the International Broadcasting Bureau (IBB) provides the administrative and engineering support for U.S. government-funded non-military international broadcast services. Broadcast elements are the Voice of America

(VOA) and Radio and TV Martí (Office of Cuba Broadcasting). In addition, the IBB provides engineering and program support to Radio Free Europe/Radio Liberty, Radio Free Asia, the Middle East Broadcasting Networks (Radio Sawa and Alhurra Television), and Radio Farda, a joint Persian-language project between VOA and Radio Free Europe.⁶

Strategic communication has generally been considered a national strategic concept, however, it is currently addressed at the theater strategic level as well.

c. History of Strategic Communication. While “strategic communication” is a fairly new term in the U.S. government lexicon, the concept, theory, and practice behind it is not. Winfield Scott recognized the importance of strategic communication at the theater level in Veracruz in 1847. Realizing the influence of the Catholic Church on Mexican society, Scott attended Mass with his staff at the Veracruz Cathedral to display the respect of U.S. forces. He further ordered U.S. soldiers to salute Mexican priests in the streets. Each of these measures was “part of a calculated campaign to win the friendship of the Mexicans.”⁷

The recent history of national strategic communication shows concerted efforts to positively portray the U.S. story in order to persuade and influence.

(1) The Committee on Public Information (1917), also known as the Creel Committee after its chief newspaperman George Creel, sought to rally U.S. public opinion behind World War I on behalf of the Wilson administration. Its focus was the domestic audience and it used public speakers, advertising, pamphlets, periodicals, and the burgeoning American motion picture industry.

(2) The Office of War Information (1942) focused both domestically and overseas, with broadcasts sent in German to Nazi Germany. The Voice of America (VOA) began its first broadcast with the statement, “Here speaks a voice from America. Everyday at this time we will bring you the news of the war. The news may be good. The news may be bad. We shall tell you the truth.”

(3) The Smith-Mundt Act (1948) (actually, “The U.S. Information and Educational Exchange Act (Public Law 402; 80th Congress)”), established a statutory information agency for the first time in a period of peace with a mission to “promote a better understanding of the United States in other countries, and to increase mutual understanding” between Americans and foreigners. The act also forbade the Voice of America to transmit to an American audience. It is worth noting that Smith-Mundt is often cited today as the basis to limit the use of government information activities to influence since it may result in “propagandizing” the American public. This, of course, is complicated by the inevitable “blowback” or “bleedover” of foreign influence activities based on the global information environment.⁸

(4) The United States Information Agency (USIA) (1953) was established by President Eisenhower as authorized by the Smith-Mundt Act. It encompassed all the information programs, including VOA (its largest element), that were previously in the Department of State, except for the educational exchange programs, which remained at State. The USIA Director reported to the President through the National Security Council and received complete, day-to-day guidance on U.S. foreign policy from the Secretary of State.

(5) A 1998 State Department reorganization occurred in response to calls by some to reduce the size of the U.S. foreign affairs establishment. (This is considered the State Department’s “peace dividend” following the Cold War). The act folded the USIA into the Department of State. It pulled the Broadcasting Board of Governors out of USIA and made it a separate organization. The USIA slots were distributed throughout the State Department and its mission was given to the Bureau of International Information Programs.

d. National Strategic Communication: Current Models and Processes. The demise of USIA is generally regarded (in retrospect) as diluting the ability of the United States to effectively promulgate a

national communication strategy, coordinate and integrate strategic themes and messages, and support public diplomacy efforts worldwide.⁹ Additionally, organizations and processes have experienced great flux in recent years. The current administration retained Presidential Decision Directive (PDD) 68 that was enacted in 1999 by the Clinton administration. PDD 68 addressed those problems when no single U.S. agency was empowered to coordinate US efforts to sell its policies and counteract bad press abroad. It directed top officials from the Defense, State, Justice, Commerce and Treasury departments as well as those from the Central Intelligence Agency and FBI to establish an International Public Information (IPI) Core Group chaired by the Under Secretary for Public Diplomacy and Public Affairs at the Department of State.¹⁰ It is evident, however that this core group is currently inactive. Other recent initiatives to coordinate and integrate national strategic communication efforts have also faltered. The White House Office of Global Communication was disbanded in 2003. A Strategic Communication Policy Coordinating Committee (PCC) met on several occasions, but then went dormant. A Muslim Outreach Policy Coordinating Committee was more active and in fact, developed a draft national communication strategy that did not make it out of the White House.¹¹ On the other hand, an Interagency Strategic Communication Fusion Team has remained an active, albeit informal, coordinating body at the action officer level. Team members share information about their respective plans and activities in order to leverage each other's communication with international publics. The team coordinates and de-conflicts the production and the dissemination of information products but does not task. Instead, team members reach across office, bureau and agency boundaries to offer or to seek support for their strategic communication plans and activities.¹²

Despite the failures in the recent past, currently ongoing actions at the national level appear encouraging. Ambassador Karen Hughes assumed duties as the Under Secretary of State for Public Diplomacy and Public Affairs in the early fall of 2005. The Under Secretary helps ensure that public diplomacy (which she describes as engaging, informing, and influencing key international audiences) is practiced in harmony with public affairs (outreach to Americans) and traditional diplomacy to advance U.S. interests and security and to provide the moral basis for U.S. leadership in the world.¹³ Ambassador Hughes has taken positive steps since taking the job. She has provided specific guidance to public affairs officers at embassies throughout the world that shortcuts (and eliminates in many cases) bureaucratic clearances to speak to the international press. She has established a rapid response unit within the State Department to monitor and respond to world and domestic events. She has reinvigorated the Strategic Communication PCC and established communication plans for key pilot countries. And she has established processes to disseminate coordinated U.S. themes and messages laterally and horizontally within the government. Finally and perhaps most importantly, a long awaited National Strategy for Public Diplomacy and Strategic Communication was published under her leadership in May 2007.

The Defense Department recognizes the problems as well. The Quadrennial Defense Review (QDR) conducted a spin off study on Strategic Communication that resulted in a roadmap addressing planning, resources and coordination. Perhaps the most important aspect of the roadmap is the stated objective of developing strategic communication plans in conjunction with policy development, thus fulfilling Edward R. Murrow's desire to be brought in on the takeoff, not the crash landing.¹⁴

Despite these recent positive initiatives, it remains to be seen whether Ambassador Hughes' efforts or those of DOD will result in adequate resourcing or processes and organizations that endure beyond the current administration.

e. Theater Strategic Communication. Theater strategic communication is an emergent concept with only brief discussion in Joint Publication 3-13. However, because of the importance of the information element of power in the current military campaigns in Iraq and Afghanistan, Combatant Commanders have established processes and organizations to address the need. An unclassified draft annex on strategic communication in the National Military Strategic Plan for the War on Terrorism¹⁵ directs Combatant Commanders to develop internal processes and, where appropriate, organizations for integrating strategic communication within Combatant Command plans and operations. This annex further indicates that Combatant Commanders, when appropriate, may identify a strategic communication director. U.S.

Central Command has established a robust strategic communication directorate; other combatant commands have not, but instead have used other models for this purpose. While national strategic communication lists principal capabilities of PA, PD and IO, DOD strategic communication (and thus combatant command strategic communication) includes military PA, defense support to public diplomacy (alternately referred to as military support to public diplomacy), aspects of IO (principally PSYOP), Military Diplomacy (MD) and Visual Information (VI).¹⁶ The concept of defense support to public diplomacy is still vaguely defined with examples ranging from theater web initiatives aimed at certain regions and demographics within those regions to theater logistical support to embassies and diplomatic staffs. Military Diplomacy includes traditional interactions between U.S. senior military leaders and foreign military leaders. Beyond the importance of theater strategic communications in ongoing military operations, emergent doctrine is correct to point out the importance of strategic communication activities in implementing theater security cooperation plans (TSCPs) based on its inherent shaping and deterrence capability.¹⁷

f. Ends, Ways, Means: Where Does Strategic Communication Fit? Strategists use a model of “ends, ways and means” to describe all aspects of a national or military strategy. Strategy is about how (the way) leaders will use the capabilities (means) available to achieve objectives (ends).¹⁸ Understanding and engaging key audiences is meant to change perceptions, attitudes, beliefs and, ultimately behaviors to help achieve military (and in turn national) objectives. Thus, parsing the QDR definition it is apparent that strategic communication is a “way” to achieve an information effect on the cognitive dimension of the information environment (the required “end”). Military leaders should not limit strategic communication means to only those primary capabilities listed in the definition. Strategic communication means should be restricted only by the requirement to achieve the desired information effect on the target audience.

In that light, messages are certainly sent by verbal and visual communications means, but they are also sent by actions. (Note that the QDR definition specifically includes “actions”). In fact, senior officials point out that strategic communication is “80% actions and 20% words.”¹⁹ Specifically, how military operations are conducted affects the information environment by impacting perceptions, attitudes and beliefs.

g. Strategic Communication and IO: A Side by Side Comparison. The current definitions of IO (Joint Publication 3-13) and Strategic Communication (QDR Strategic Communication Roadmap) are clear and fairly distinct to the fully engaged information practitioner, but there are nuances that make those distinctions difficult to grasp for others (to include operational commanders) and so clarifying these concepts is well worth considering. Strategic communication is the more broadly overarching concept targeting *key audiences* and focusing on the cognitive dimension of the information environment. IO as an integrating function, on the other hand, more specifically targets an *adversary’s decision making capability* which may be in the cognitive, informational and/or physical dimensions of the information environment.

	Target	Effect	Dimension	Primary Capabilities
SC	Key audiences (friendly, neutral, adversarial)	Understand and engage	Cognitive (people)	PA, PSYOP, MD, DSPD, VI
IO	Adversarial human and automated decision-making	Influence, disrupt, corrupt, or usurp	Cognitive, information, physical (people, processes, systems)	EW, CNO, OPSEC, MILDEC, PSYOP

Considering the targets and effects described above, it should be clear that both strategic communication and IO can be employed at all levels of warfare (tactical, operational, theater strategic and national

strategic). Tactical commanders routinely employ strategic communication in Iraq today based on their interactions with key audiences in their area of responsibility to a potential strategic end. On the other end of the scale, IO could certainly be employed strategically as part of a shaping Phase 0 operation or a deterrent Phase 1 operation against a potential adversary's decision-making capability.

h. Effectively Integrating Strategic Communication in Military Planning. Remembering that strategic communication is a way to achieve cognitive information effects using any means available takes the mystery out of the concept. Strategic communication simply employs capabilities (limited only to the imagination) to support the achievement of a military objective. Just as a commander integrates air, land and sea capabilities into military planning and execution, he can and should integrate strategic communication capabilities. The planning process is not new. The focus on and understanding of this new concept and its capabilities, however, may be.

First, planners must define the information environment and its physical, informational and cognitive dimensions. How does the target audience receive their information (TV, radio, internet, rumor, religious services, etc.)? How does culture play into the message? Who are the credible messengers? Next, planners need to consider the desired effect on the cognitive dimension, i.e. the ends or outcome. Does the endstate include changing perceptions, influencing people, gaining acceptance, gaining credibility and trust, gaining support? This will drive how the operation will be conducted where themes and messages are necessary, but not sufficient.

Any military planner will quickly see how this logical thought process fits neatly into the established military decision-making process (or campaign planning process). The information environment is considered in the analysis of the overarching operational environment. The commander's intent establishes an endstate. This must include a statement of the desired information environment endstate. A properly stated information endstate in the commander's intent will guide staffs in the selection of appropriate courses of action and drive subordinate units in the way they conduct operations to achieve that endstate. A selected course of action will then be wargamed using the traditional friendly action, expected enemy reaction, and friendly counteraction methodology. The wargaming process must also occur with an eye toward information effects. This becomes especially important in counterinsurgency operations where the enemy uses information as an asymmetric strategic means and where changing indigenous populations' perceptions can turn them from a neutral position to one in favor of coalition forces. But it also applies across all levels of the spectrum of conflict in an environment where military operations will likely be covered in real time by both mainstream and "new" media sources.

i. In Conclusion. Strategic Communication is simply a way to affect perceptions, attitudes and beliefs of key audiences in support of objectives. Certainly communications means are very important in ultimately achieving those desired information effects. But *how* military operations are conducted (or policy is implemented) is also a key component of strategic communication, since actions send very loud and clear messages. Effective strategic communication requires an organizational culture attuned to the information environment and a recognition that strategic communication, as a way to achieve information effects, consists of many capabilities (means) that are an integral part of the commander's arsenal.

Professor Dennis Murphy
Information in Warfare Group
Center for Strategic Leadership
U.S. Army War College

Updated: October 2007

¹ Reagan, Ronald. National Security Decision Directive 130. Washington, D.C.: The White House, 6 March 1984. Available from <http://www.fas.org/irp/offdocs/nsdd/nsdd-130.htm>. Internet. Accessed 18 October 2007.

² Emergent NATO doctrine on Information Operations cites Diplomatic, Military and Economic activities as “Instruments of Power.” It further states that Information, while not an instrument of power, forms a foundation as all activity has an informational backdrop.

³ Neilson, Robert E. and Daniel T. Kuehl, “Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program. National Security Strategy Quarterly (Autumn 1999): 40.

⁴ Various definitions of strategic communication exist. As of this writing, DOD is still debating the definition. The one shown here is taken from Department of Defense, QDR Execution Roadmap for Strategic Communication, (Washington, DC: U.S. Department of Defense, 25 September 2006), 3.

⁵ U.S. Department of Defense. DOD Dictionary. Available from <http://www.dtic.mil/doctrine/jel/doddict/data/p/04372.html>. Internet. Accessed 18 October 2007.

⁶ The United States Government’s International Broadcasting Bureau. Available from: <http://www.ibb.gov>. Internet. Accessed 18 October 2007.

⁷ Eisenhower, John S.D. Agent of Destiny: The Life and Times of General Winfield Scott. New York: The Free Press, 1997, 245-6.

⁸ The Smith-Mundt Act is still in effect to include the requirement not to “target” U.S. audiences. The current information environment with ubiquitous, world-wide media outlets, satellite communications and real-time reporting makes it difficult to target foreign audiences without exposing U.S. audiences to the message, however...a fact not envisioned in 1948 when the act became effective and one that continues to cause friction between the military and media.

⁹ Kaplan, David E. “Hearts, Minds, and Dollars.” *U.S. News and World Report*, 25 April 05, 25, 27.

¹⁰ Federation of American Scientists. Intelligence Resource Program. *U.S. International Public Information (IPI)*. Presidential Decision Directive PDD68, 30 April 1999. Available from <http://www.fas.org/irp/offdocs/pdd/pdd-68.htm>. Internet. Accessed 18 October 2007.

¹¹ U.S. General Accounting Office. U.S. Public Diplomacy. Washington, D.C.: U.S. General Accounting Office, April 2005. 10-13.

¹² Interagency Strategic Communication Fusion Team. Meeting summary, 27 October 2006, 4.

¹³ U.S. Department of State. Senior Officials: Under Secretary for Public Diplomacy and Public Affairs -- Karen Hughes. Available from <http://www.state.gov/misc/19232.htm>. Internet. Accessed 18 October 2007.

¹⁴ QDR Execution Roadmap for Strategic Communication, 3.

¹⁵ U.S. Department of Defense. National Military Strategic Plan for the War on Terrorism, Strategic Communication (DRAFT): Annex H. Washington, D.C.: U.S. Department of Defense, 18 April 2005.

¹⁶ QDR Execution Roadmap for Strategic Communication, 2.

¹⁷ Joint Publication 3-13, I-13.

¹⁸ Yarger, Harry R., “Toward a Theory of Strategy: Art Lykke and the Army War College Strategy Model,” *U.S. Army War College Guide to National Strategy and Policy*, June 2006, p. 107.

¹⁹ The author has attended numerous briefings by the Deputy Assistant Secretary of Defense for Joint Communication (DASD (JC)) and his staff where this has been stated. Note: the DASD (JC) is responsible for the DOD Strategic Communication Roadmap.

National Strategy and Agencies

Included in this section are descriptions of the U.S. National Strategy for Public Diplomacy and Strategic Communication & the National Security Agency

U.S. National Strategy for Public Diplomacy and Strategic Communication

The National Strategy for Public Diplomacy and Strategic Communication was published 31 May 2007. The complete document is at:

http://uscpublicdiplomacy.org/pdfs/stratcommo_plan_070531.pdf

The strategy focuses on three key strategic objectives that govern America's communication with foreign audiences: The United States should offer a positive vision of hope and opportunity to the world; isolate and marginalize violent extremists and; nurture common interests and values between Americans and foreign publics.

In addition to the three strategic objectives above the new strategy aims to support achievement of the National Security Strategy Objectives. Public diplomacy and strategic communication should always strive to support our nation's fundamental values. All communication and public diplomacy should (1) underscore our commitment to freedom, human rights and the dignity and equality of every human; (2) reach out to those who share our ideals; (3) support those who struggle for freedom and democracy; and (4) counter those who espouse ideologies of hate and oppression.

Strategic audiences are (1) Key Influencers -- those whose views can have a ripple effect throughout society. They include clerics, educators, journalists, women leaders, business and labor leaders, political leaders, scientists and military personnel. (2) Vulnerable Populations -- those groups most vulnerable to extremist ideology, like youth and women and girls as well as minorities. (3) Mass Audiences -- the United States must expand its presence on international broadcasts and rapidly develop improved capabilities to employ the power of Internet and other new technologies.

Public diplomacy priorities are programs and activities that expand education and exchange programs, modernize communications, and promote the "diplomacy of deeds". The Policy Coordinating Committee (PCC) on Public Diplomacy and Strategic Communication led by the Under Secretary for Public Diplomacy and Public Affairs is the overall mechanism to coordinate our public diplomacy across the interagency community. To accomplish this, the PCC will establish the following structures: (1) Counterterrorism Communications Center headquartered at the Department of State, with the core mission of developing messages and strategies to discredit terrorists and their ideology; (2) the Interagency Crisis Communication Team -- the National Security Council will initiate an interagency conference call immediately upon major breaking news that might have an impact on our efforts against violent extremism to coordinate message points; (3) Regular Monitoring of Implementation of the strategy.

The strategy directs that each agency and embassy should develop its own specific plan to implement the objectives of the document. It also gives guidance that each agency's plan should identify two or three key programs/policies which the agency will highlight to support the overall public diplomacy/strategic communication goals, identify target audiences, assign responsibility and outline specific plans for communicating key programs, and policies to the target audiences through speeches, foreign travel, media interviews, etc.. Additionally, each agency must identify NGO and private sector partners with whom the agency works, subject matter experts who can explain and advocate U.S. policy, and workers who speak foreign languages and could translate/participate in interviews. Each agency must also recommend envoys to advance public diplomacy efforts, outline current activities and programs that can be linked to support global public diplomacy, and develop criteria to evaluate effectiveness.

The new strategy recognizes the importance of basic information sharing. To support this, the State Department has created a new "Public Diplomacy Briefing Book" that is available via the internet to update all USG officials on regional and country-specific policies, official statements and key messages, compelling stories, provide a database of images and videos, and information that represents mainstream Muslim views and rejection of terrorist/extremism. Additionally, best practices will be identified and shared through agency websites.

Further it recognizes the importance of audience analysis: Understanding foreign public opinion is vital to successful communication. The USG should create a central repository of information and analysis of public opinion in different countries so we can better understand how citizens of other countries view us and what values and interests we have in common.

Proactive media booking is directed. The State Department's new regional media hubs in London, Brussels and Dubai are equipped to support messaging and booking of senior USG officials abroad to project American viewpoints.

CONCLUSION

Public diplomacy is, at its core, about making America's diplomacy public and communicating America's views, values and policies in effective ways to audiences across the world. Public diplomacy promotes linkages between the American people and the rest of the world by reminding diverse populations of our common interests and values. Some of America's most effective public diplomacy is communicated not through words but through our deeds, as we invest in people through education, health care and the opportunity for greater economic and political participation. Public diplomacy also seeks to isolate and marginalize extremists and their ideology. In all these ways, public diplomacy is "waging peace," working to bring about conditions that lead to a better life for people across the world and make it more difficult for extremism to take root.

There are five attachments to the plan:

Attachment A: ACTION PLAN FOR STRATEGIC OBJECTIVES

Attachment B: GENERAL COMMUNICATION GUIDELINES.

Attachment C: CORE MESSAGES

Attachment D: ADDITIONAL COMMUNICATION VEHICLES.

Attachment E: EVALUATION AND ACCOUNTABILITY.

Updated: October 2007

National Security Agency (NSA)



National Security Agency/Central Security Service (NSA/CSS)

Introduction

The ability to understand the secret communications of our adversaries while protecting our own communications – a capability in which the United States (U.S.) leads the world – gives our nation a unique advantage.

Executive Order No. 12333, dated December 4, 1981, describes the responsibilities of the NSA/CSS in more detail. The resources of the NSA/CSS are organized for the accomplishment of two national missions:

The Signals Intelligence (SIGINT) mission allows for an effective, unified organization and control of all foreign signals collection and processing activities of the U.S. The NSA/CSS is authorized to produce SIGINT in accordance with the objectives and priorities established by the Director of National Intelligence in consultation with the President's Foreign Intelligence Advisory Board.

The Information Assurance (IA) mission provides the solutions/services and conducts Defensive Information Operations (DIO) to protect information processed by U.S. national security systems. The intent is to measurably improve the security of critical operations and information by providing know-how and technology to our suppliers, partners and clients, when and where they need them.

The NSA/CSS is America's cryptologic organization. It produces foreign signals intelligence and performs highly specialized activities to protect U.S. Government national security information systems. A high technology organization, the NSA/CSS is on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the U.S. Government. It is said to be the largest employer of mathematicians in the U.S. and perhaps the world. Its mathematicians design cipher systems that search for weaknesses in adversaries' systems/codes and that protect the integrity of U.S. systems.

SIGINT is a unique discipline with a long and storied past. Its modern era dates to World War II, when the U.S. broke the Japanese military code and learned of plans to invade Midway Island. This intelligence allowed the U.S. to defeat Japan's superior fleet. The use of SIGINT is believed to have directly contributed to shortening the war by at least one year. Today, SIGINT continues to play an important role in keeping the United States a step ahead of its enemies.

The IA mission becomes increasingly more challenging as the world becomes more technology-oriented. IA professionals go to great lengths to make certain that Government systems remain impenetrable. The NSA/CSS supports the highest levels of the U.S. Government to the war fighter.

The NSA/CSS conducts one of the U.S. Government's leading Research and Development (R&D) programs. Some of the Agency's R&D projects have significantly advanced the state of the art in the scientific and business worlds. The NSA/CSS's early interest in cryptanalytic research led to the first large-scale computer and the first solid-state computer, predecessors to modern computing. The NSA/CSS also made ground-breaking developments in semiconductor technology and remains a world leader in many technological fields.

Technology and the world change rapidly, and great emphasis is placed on staying ahead of these changes with employee training programs. The National Cryptologic School is indicative of the Agency's commitment to professional development. The school not only provides unique training for the NSA workforce, but it also serves as a training resource for the entire Department of Defense (DoD). The NSA/CSS sponsors employees for bachelor and graduate studies at the Nation's top universities and colleges, and selected Agency employees attend the various war colleges of the U.S. Armed Forces.

Most NSA/CSS employees, both civilian and military, are headquartered at Fort Meade, Maryland, centrally located between Baltimore, MD and Washington, D.C. Its workforce represents an unusual combination of specialties: analysts, engineers, physicists, mathematicians, linguists, computer scientists, researchers, as well as customer relations specialists, security officers, data flow experts, managers, administrative officers and clerical assistants.

SIGINT Mission

The NSA/CSS collects, processes and disseminates foreign SIGINT. The old adage that "knowledge is power" has perhaps never been truer than when applied to today's threats against our nation and the role SIGINT plays in overcoming them.

The NSA/CSS's SIGINT mission protects the nation by: Providing information in the form of SIGINT products and services that enable our government to make critical decisions and operate successfully; Protecting the rights of U.S. citizens by adhering to the provisions of the 4th amendment to the Constitution and; Using the nation's resources responsibly, according to the best management processes available.

Other Intelligence Community (IC) agencies are responsible for other types of intelligence: Central Intelligence Agency (CIA) - Human Intelligence (HUMINT); Defense Intelligence Agency – HUMINT and Measurement and Signature Intelligence (MASINT) and; National Geospatial Agency (NGA) – Imagery Intelligence

These different yet complementary disciplines give our nation's leaders a greater understanding of the intentions of our enemies.

The NSA/CSS's SIGINT mission provides our military leaders and policy makers with intelligence to ensure our national defense and to advance U.S. global interests. This information is specifically limited to that on foreign powers, organizations or persons and international terrorists. The NSA/CSS responds to requirements levied by intelligence customers, which includes all departments and levels of the U.S. Executive Branch of Government.

The prosecution of the SIGINT mission has evolved from the relatively static, industrial age, Cold War communications environment to the ubiquitous, high speed, multi-functional technologies of today's information age. The ever-increasing volume, velocity and variety of today's communications make the

production of relevant and timely intelligence for military commanders and national policy makers more challenging than ever.

As much as modern telecommunications technology poses significant challenges to SIGINT, the many languages used in the nations and regions of the world that are of interest to our military and national leaders require the NSA/CSS to maintain a wide variety of language capabilities. Successful SIGINT depends on the skills of not only language professionals but those of mathematicians, analysts, and engineers, as well. The nation is indebted to them for the successes they have won.

IA Mission

IA is one of the two core missions of the NSA/CSS. The Information Assurance Directorate (IAD) is dedicated to providing IA solutions that will keep U.S. national security systems safe from harm.

IA refers to the measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

The IAD's mission involves detecting, reporting, and responding to cyber threats; making encryption codes to securely pass information between systems; and embedding IA measures directly into the emerging DoD's Global Information Grid (GIG). It includes building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions. It entails testing the security of customers' systems, providing Operations Security (OPSEC) assistance, and evaluating commercial software and hardware against nationally set standards to better meet our nation's needs.

The IAD's mission has evolved through three very distinct stages: Communications Security (COMSEC), Information Systems Security (INFOSEC), and IA. Following World War II and the Korean War, efforts focused primarily on cryptography (i.e. designing and building encryption devices to provide confidentiality for information). COMSEC is defined as the measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emission security, and physical security of COMSEC material.

In the 1980s, the introduction and widespread use of computers created new demands to protect information exchanges between interconnected computer systems. This demand created the Computer Security (COMPUSEC) discipline. However, the community recognized that stand-alone COMSEC and COMPUSEC activities could not protect information during storage, processing or transfer between systems. This recognition gave rise to the term INFOSEC and the information protection mission took on a broader perspective. INFOSEC is defined as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

In the 1990s, IA emerged and focused on the need to protect information during transit, processing, or storage within complex and/or widely dispersed computers and communication system networks. IA also includes a dynamic dimension where the network architecture is itself a changing environment, including the information protection mechanisms and features that detect attacks and enable a response to those attacks. IA measures protect against the exploitation or penetration efforts routinely conducted by sophisticated adversaries, but also protect against hackers or criminals from creating havoc across layered domains.

Today, IA incorporates more than just the need for confidentiality achieved through the use of encryption products that the NSA/CSS produces or certifies. IA also includes the DIO elements that protect and defend information and information systems.

Contact Information: Community Outreach Office (410) 854-0903

Website: <http://www.nsa.gov/>

Updated: November 2007

Department of Defense Directives and Roadmaps

Included in this section are the DoD Directive (DoDD) O-36600.01 *Information Operations*; the *Information Operations (IO) Roadmap, 2003*; and the *2006 Quadrennial Defense Review (QDR) Execution Roadmap for Strategic Communication*.

Department of Defense Directive (DoDD) O-3600.01 Information Operations



This section presents a synopsis of non-restricted information from the current Department of Defense Directive.

Purpose. Department of Defense Directive (DoDD) 3600.1, "Information Operations" (FOUO) is the *fundamental* document for both understanding and employing Information Operations (IO). As such it should be the starting point for all study of Information Operations as undertaken by U.S. practitioners. It gives policy guidance to the Department of Defense for the management and implementation of IO throughout DoD, sets out responsibilities for the key offices at OSD and joint command levels and gives definitions to key terms.

Scope. As policy guidance, it defines terms; assigns responsibilities to officials, services, unified commands, and agencies; and provides the basis for the development of joint and service doctrine for IO. The term, "doctrine", as defined by Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms" (October, 2004) means: "*Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application*".

Information Operations (IO) Defined. IO is "The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own".

Use of IO. IO is to be employed to support full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information, to affect adversary decision cycles with the goal of achieving information superiority for the United States.

Core IO Capabilities.

IO employs five core capabilities to achieve desired Combatant Commander effects or prevent the enemy from achieving his desired effects: *EW, CNO, PSYOP, MILDEC, and OPSEC*. They are operational in a direct and immediate sense; they either achieve critical operational effects or prevent the adversary from doing so. They are interdependent and increasingly need to be integrated to achieve desired effects.

Supporting Capabilities (See Glossary for definitions):

- Counterintelligence
- Physical (kinetic) attack
- Physical Security
- Information Assurance (IA)
- Combat Camera

Related Capabilities. (See Glossary for definitions):

- Public Affairs (PA)
- Civil-Military Operations (CMO)
- Defense Support to Public Diplomacy (DSPD)

Intelligence Support. Intelligence will be developed, consistent with the National Intelligence Priorities Framework, to provide data about adversary information systems or networks; produce political-military assessments; conduct human factors analysis; and provide indications and warning of adversary IO, including threat assessments.

RESPONSIBILITIES. The following officials, commands, and agencies are tasked with the specific responsibilities indicated:

Under Secretary of Defense for Intelligence (USD(I)) :

- Serve as the Principal Staff Assistant to the Secretary of Defense for IO.
- Develop and oversee DoD IO policy and integration activities.
- Assess performance/responsiveness of DoD and Military Intelligence activities to support IO.
- Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements.
- Establish specific policies for the development and integration of CNO, MILDEC and OPSEC as core IO capabilities.

Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) :

- Establish specific policies for the development and integration of EW as a core IO capability.
- Develop and maintain a technology investment strategy for development, acquisition, and integration of EW capabilities.
- Invest in and develop the science and technologies needed to support IO capabilities.

The Under Secretary of Defense for Policy (USD(P)):

- Provide DoD oversight of IO planning, execution, and related policy guidance including the establishment of an OSD review process to assess IO plans and programs

- Lead interagency coordination, exclusive of the IC, and international cooperation involving planning and employment of IO capabilities.
- Establish specific policy and oversight for development and integration of PSYOP as a core IO capability and DSPD as a related capability.

The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) :

- Develop policy and procedures on matters pertaining to the establishment and management of an IO career force in coordination with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the USD(P), the USD(I), and others, as appropriate.
- Provide training policy and oversight as it pertains to the integration of all IO capabilities into joint exercises and joint training regimes.

The Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO) will:

- Establish specific policy for the development and integration of IA and Computer Network Defense (CND) as related to CNO as a core IO capability.
- Oversee and assess the efforts of the Heads of the DoD Components to plan, program, develop, and field IA and CND capabilities in support of CNO.

Assistant Secretary of Defense for Public Affairs will:

- Establish specific policy for the relationship of PA to IO.
- Oversee PA planning and coordination efforts as related to IO within DoD
- Oversee the development and conduct of appropriate training and education that defines PA's relationship to IO for public affairs and visual information personnel at the Defense Information School.

Commander, U.S. Strategic Command (CDRUSSTRATCOM):

- Integrate and coordinate DoD IO core capabilities that cross geographic areas of responsibility or core IO areas.

Commander, U.S. Special Operations Command (CDRUSSOCOM)

- Integrate and coordinate DoD PSYOP capabilities to enhance interoperability and support USSTRATCOM's information operations responsibilities and other combatant commanders' PSYOP planning and execution.
- Support the other Combatant Commanders through joint employment of PSYOP and other special operations force IO capabilities.
- Employ other special operations force IO capabilities as directed.

The Secretaries of the Military Departments and CDRUSSOCOM:

- Develop IO doctrine and tactics, and organize, train, and equip for IO for their Title 10 (U.S. Code) and Major Force Program responsibilities.

The Chairman of the Joint Chiefs of Staff

- Serve as the principal military advisor to the President of the United States, the National Security Council, and the Secretary of Defense on IO.
- Validate capability-based IO requirements through the Joint Requirements Oversight Council.

- Develop and maintain joint doctrine for core, supporting, and related IO capabilities in joint operations.
- Ensure all joint education, training, plans, and operations include, and are consistent with, IO policy, strategy, and doctrine.

Definitions. See Glossary for definitions of the following terms: Computer Network Attack, Computer Network Defense, Computer Network Exploitation, Computer Network Operations, Defense Support to Public Diplomacy, Electronic Warfare, Human Factors, Information, Information Assurance, Information Operations Specialists and Planners, Information Superiority, Information System, Military deception, Operations Security, Psychological Operations, Public Affairs, and Public Diplomacy.

Final Department of Defense Directives (DoDD) on line:

DoDD 1000.1 thru 4999.99 -- <http://www.dtic.mil/whs/directives/corres/dir1.html>

DoDD 5000.1 thru 8999.99 -- <http://www.dtic.mil/whs/directives/corres/dir2.html>

Last Updated: October 2007

The Information Operations (IO) Roadmap, 2003



This section provides an UNCLASSIFIED synopsis of those unclassified elements of the Road Map.

Persons who are, or will become Information Operations (IO) practitioners, should read this fundamentally important document in its entirety, and become familiar with its critiques and its proposals for improvement. A redacted version of the document, removing those items still classified, can be accessed at the following George Washington University website:

www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf

The classified, 74-page, "IO Roadmap" discusses specific issues and deficiencies related to the five core IO capabilities (*PSYOP*, *Computer Network Operations*, *Military Deception*, *OPSEC*, and *Electronic Warfare*), the related DoD capabilities (Public Affairs and Civil Military Operations), and the several supporting capabilities. It addresses shortcomings in doctrine, organizational structure, and practice, it gives twelve general recommendations for improvement (see below), and it also states more than forty specific recommendations for further action.

Purpose. The Secretary of Defense, in his introduction to the Roadmap states that it seeks to advance the goal of Information Operations becoming a core military capability of U.S. forces. The current Roadmap edition (30 October 2003) aims to provide a framework for understanding Information Operations and to present a critique of the current state of IO. The Roadmap calls for a dedicated workforce, as well as development of new organizational structures that will enhance IO, and also support Defense Transformation efforts

Three IO Functional Areas. The Roadmap broadly defines three integrated functional areas that include the five IO core capabilities, as follows:

1. Those activities aimed at deterring, discouraging, dissuading, and directing an adversary, thereby disrupting his unity of command and purpose while preserving our own (*PSYOP*).
2. Protecting our plans while misdirecting theirs, thereby allowing our forces to mass their effects to maximum advantage while the adversary expends his resources to little effect (*OPSEC* and *Military Deception*).
3. Control adversarial communications networks while protecting ours (*Electronic Warfare* and *Computer Network Operations*).

The plan calls for extensive IO preparations in peacetime using the full range of intelligence, surveillance, and reconnaissance capabilities to accurately map the computer networks and electronic signatures of potential adversaries. It calls for large efforts to characterize adversarial audiences as well as the adversarial decision makers themselves, in order to better target and exploit these using IO capabilities.

The Roadmap identifies the following benefits that will be accrued if its recommendations are achieved:

- Development of a common IO lexicon.
- More execution authority delegated to combatant commanders.
- Development of a trained and educated professional career force for IO.
- Centralized IO planning, integration, and analysis support from STRATCOM.
- Enhanced IO capabilities for the warfighter, to include:
 - Improved ability to disseminate powerful messages in support of adversary behavior modification.
 - Protection of networks with a real defense in depth strategy.
 - A robust offensive suite of capabilities to include full range electronic and computer network attack, with increased reliability through improved command and control, assurance testing, and refined tactics and procedures.

Critiques of Current State of Information Operations. The discussion of challenges and shortcomings in the Information Operations area include the following:

- No consensus on the definition of Information Operations or its contribution to overall mission accomplishment.
- Electronic Warfare policy and plant investment are outdated.
- OPSEC planning process is not widely applied and OPSEC, itself, is largely an “afterthought”. Military Deception staffs are not adequately trained prior to their assignments.
- Relationship of Public Affairs, Public Diplomacy, and PSYOP must be studied and clarified. PA must become more proactive. PSYOP authorities must be further decentralized.
- Information Operations career force and education require better planning and coordination for development.

Roadmap General Recommendations: The Roadmap’s twelve recommendations are as follows:

1. Approve a common understanding of Information Operations.
2. Consolidate oversight and advocacy for Information Operations.
3. Delegate capabilities to combatant commanders.
4. Create a well trained and educated career work force.
5. Provide consolidated and comprehensive analytical support.
6. Correct immediate shortfalls and develop a long term defense in depth strategy for CND.
7. Mature CNA into a reliable warfighting capability.
8. Develop an electronic warfare investment strategy.

9. Increase psychological operations capabilities.
10. Clarify lanes in the road for PSYOP, Public Affairs, and Public Diplomacy.
11. Assign advocacy for operations security and military deception.
12. Improve transparency of Information Operations planning, programming, and budgeting, and execution system.

Policy Actions to Implement the Roadmap to Date:

- IO Advocacy. DoDI 5143.01, “Undersecretary of Defense for Intelligence”, issued 23 November 2005, designates the USD(I) as the principal staff assistant to the Secretary of Defense for Information Operations policy and integration activities.
- IO Career Force. DoDI 3608.11, “Information Operations Career Force” issued 4 November 2005 implemented the following:
 - Designated the Undersecretary of Defense for Intelligence (USD (I)) as the functional proponent for the IO career force
 - Specified that an interim IO career force of active and reserve military personnel be established, consisting of two categories of position: IO Planners and IO Capability Specialists (see glossary for definitions).
 - Allow for creation of guidance for enlisted and civilian IO career force in the future.
 - Required the USD (I) to monitor the accession, retention, and promotion rates for the IO career force.
- IO Education. DoDI 3608.12, “Joint Information Operations Education”, (4 November 2005):
 - Specified that Joint IO education programs support the transformation of IO into a core military capability
 - Joint IO planners courses and graduate education programs expand the IO knowledge base in the services.
 - Designates USSTRATCOM as the operational advocate for joint IO education.
 - Requires National Defense University to have the Joint Forces Staff College (Norfolk, VA) develop and conduct a Joint IO Planner’s Course.
 - Requires the Naval Postgraduate School (Monterey, CA) to establish an IO Center of Excellence and establish a graduate level joint IO education program.

DoD directives (DoDD) and instructions (DoDI) are available on line at:

www.dtic.mil/whs/directives/

Chairman of the Joint Chiefs of Staff instructions (CJCSI) and directives (CJCSD) are on line at:

www.dtic.mil/cjcs_directives/index.htm

Last Updated: October 2007

This Page Intentionally Blank

QDR Execution Roadmap for Strategic Communication



***This section provides a synopsis of the 2006 Quadrennial Defense Review (QDR)
Execution Roadmap for Strategic Communication***

The QDR Execution Roadmap for Strategic Communication was signed by Deputy Secretary of Defense Gordon England on 25 September 2006.

Purpose: The purpose of the QDR Execution Roadmap is to provide guidance for implementing Strategic Communication direction for the 2006 Quadrennial Defense Review (QDR). It includes a plan of action and milestones (POA&AM) which assigns objectives tasks, and milestones, with associated offices of Primary Responsibility (OPR). The roadmap also provides an initial estimate of the costs of improving capabilities that support Strategic Communication and provides senior leadership with a mechanism to advance high priority issues for decision through the Fiscal Years (FY) 2008-2013. The Roadmap identified important actions and leads for each of 55 tasks identified. Approximately 35 tasks that were to be completed within a year of the publication of the Roadmap

Statement of the Problem: The Roadmap stated that the problem was that the U.S. military is not sufficiently organized, trained or equipped to analyze, plan, coordinate and integrate the full spectrum of capabilities available to promote America's interests as part of a national effort to improve the integration of information as a vital element of national power. The current changes in the global information environment require the Department of Defense (DoD), in conjunction with other U. S. Government (USG) agencies, to implement more deliberate and well-developed strategic communication processes.

Definition of Strategic Communication: The Roadmap defined Strategic Communication as: "Focused United States Government processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power."

Goal: DoD will increase its effectiveness in strategic communication by developing a culture that recognizes the value of communication and integrates communication considerations into policy development, operational planning, execution, and assessment to advance national interests.

Objectives. The Roadmap defined three objectives for achieving DoD's goal of effective strategic communication:

Objective 1. Institutionalize a DoD process by which principles of strategic communication are incorporated in the development of strategy, policy formulation, planning, and execution.

Two major tasks identified in support of institutionalizing the DoD process include facilitating horizontal integration of strategic communication within DoD and improving the integration of the DoD's strategic communication process with the strategic communication process of the U.S. Government.

To help the internal DoD integration the Roadmap directed the establishment of DoD Strategic Communication Integration Group (SCIG) that will provide recommendations to integrate strategic communication throughout OSD, the Joint Staff, Combatant Commands, Military departments and other elements of DoD. Further, it directed the creation of a DoD Strategic Communication Secretariat staffed with personnel from OSD, Joint Staff, and included Military Department Liaisons, to support the DoD SCIG.

To improve the integration with the U.S. Government strategic communication process the Roadmap directed the Undersecretary of Defense for Policy (USD(P)), in coordination with the Assistant Secretary of Defense for Public Affairs to begin conferences within DoD and follow on conferences with Department of State (DOS) and to develop a formal process to coordinate and synchronize DoD strategic communication activities with key allies and coalition partners.

Objective 2. Define roles, responsibilities and relationships, and develop doctrine for strategic communication and its primary communication supporting capabilities: Public Affairs (PA); aspects of Information Operations (IO), principally PSYOP; Visual Information (VI) and the DoD activities of Military Diplomacy (MD), and Defense Support to Public Diplomacy (DSPD). To accomplish this objective, the Roadmap directed the development of DoD Directive on strategic communication and on military diplomacy, and Chairman Joint Chief of Staff Instructions on defense support to public diplomacy plus a review of other DoD Directives, Instructions and Publications for strategic communication implications.

Objective 3. Properly resource Military Departments and Combatant Commands to organize, train, and equip DoD's primary communication supporting capabilities. In order to accomplish this objective, the Roadmap described tasks to be accomplished to include the development of concept of operations (CONOPS) for the Joint Public Affairs Support Element (JPASE), Joint Psychological Operations Support Element (JPSE), as well as a CONOPS for VI. Additional tasks were identified along with projected FY 08 and future FY impact in dollar amounts needed to accomplish the task.

Last Updated: November 2007

Department of Defense Organizations



Included in this sections descriptions of the following organizations:

Under Secretary of Defense – Policy (USD(P))

Under Secretary of Defense for Intelligence

Assistant Secretary of Defense – Networks and Information Integration (ASD(NII))

DoD Strategic Communication Integration Group (SCIG)

Defense Information Systems Agency (DISA)

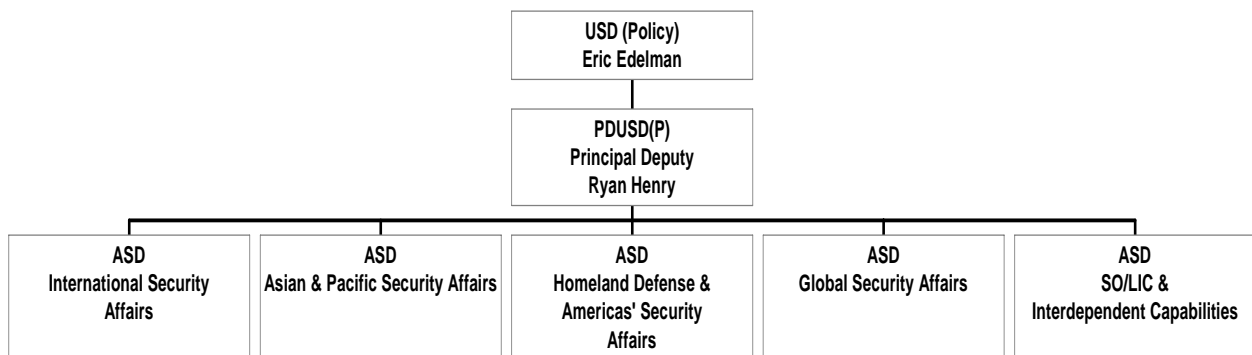
Information Assurance Technology Analysis Center (IATAC)

This Page Intentionally Blank

Under Secretary Of Defense – Policy (USD(P))



Mission: USD(P) is the principal staff assistant and advisor to the SecDef for all matters concerning the formation of national security and defense policy and the integration and oversight of DoD policy and plans to achieve national security objectives. The USD(P) oversight and policy responsibilities include the IO core capability of PSYOP, and the related capability of Civil Military Affairs, both of which fall within the oversight responsibilities of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict and Interdependent Capabilities. The Office of the USD(P) is organized as follows:



The directed responsibilities of the USD(P) include but are not limited to the following:

- Represent the Department of Defense, as directed, in matters involving the National Security Council (NSC); the Department of State; and the other Federal Departments, Agencies, and inter-Agency groups with responsibility for national security policy.
- Serve as a member of the NSC Deputies Committee; serve as a member of the Deputies Committee for Crisis Management; and advise the Secretary of Defense on crisis prevention and management, including contingency planning for major areas of concern.
- Develop DoD policy guidance, provide overall supervision, and provide oversight of planning, programming, budgeting, and execution of special operations activities, including civil affairs and psychological operations, and of low-intensity conflict activities, including counter-terrorism, support to insurgency, and contingency operations.
- Develop policy and provide oversight for emergency planning and preparedness, crisis management, defense mobilization in emergency situations, military support to civil authorities, civil defense, and continuity of operations and government. Develop policy and coordinate DoD participation in, and

exercise staff supervision over, special activities, special access programs, sensitive support to non-DoD agencies, and the joint worldwide reconnaissance schedule.

Principal Deputy Undersecretary of Defense for Policy – PDUSD(P)-- Provides advice and assistance to the Secretary of Defense, Deputy Secretary of Defense and the Under Secretary of Defense for Policy on national security policy, military strategy, and defense policy.

The Assistant Secretary of Defense for International Security Affairs – The principal staff assistant and advisor to the Under Secretary of Defense for Policy and the Secretary of Defense for formulating international security and political-military policy for Africa, Asia-Pacific, Near-East and South Asia, and the Western Hemisphere. He also provides policy oversight for security assistance and prisoner of war (POW)/missing in action (MIA) issues.

The Assistant Secretary of Defense for Asian and Pacific Security Affairs - The office of Asian and Pacific Affairs Security Affairs is responsible for U.S. security and defense policy in the Asia-Pacific region.

The Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs – the following offices fall under the ASD for Homeland Defense and Americas' Security Affairs:

- Office of the Deputy Assistant Secretary of Defense for Homeland Defense
- Office of the Deputy Assistant Secretary of Defense for Western Hemisphere Affairs
- Office of Deputy Assistant Secretary of Defense for Homeland Security Integration
- Office of Deputy Assistant Secretary of Defense for Crisis Management & Defense Support to Civil Authorities

The responsibilities of the ASD for Homeland Defense & Americas Security Affairs are best described by going to the web page http://www.defenselink.mil/policy/sections/policy_offices/hd/index.html -

The Assistant Secretary of Defense for Global Affairs – the following offices and responsibilities fall under the ASD for Global Affairs:

- Defense Technology Security Administration (DTSA)
- Freedom of Navigation: FY 2006 OPERATIONAL ASSERTIONS
- Freedom of Navigation: FY 2005 OPERATIONAL ASSERTIONS
- Freedom of Navigation: FY 2004 Operational Assertions
- Freedom of Navigation: FY 2000 - 2003 OPERATIONAL ASSERTIONS
- Office of the Assistant Secretary of Defense for Counter Narcotics, Counter Proliferation, and Global Threats
- Office of the Deputy Assistant Secretary of Defense for Prisoners of War & MPA
- Office of the Deputy Assistant Secretary of Defense for Partnership Strategy
- Office of the Deputy Assistant Secretary of Defense for Detainee Affairs
- Office of the Deputy Assistant Secretary of Defense for Threat Security Policy
- Defense Security Cooperation Agency
- Regional Defense Combating Terrorism Fellowship Program

The responsibilities for each office under the ASD for Global Affairs are best described by going to the web page: http://www.defenselink.mil/policy/sections/policy_offices/index.html

The Assistant Secretary of Defense for Special Operations/Low Intensity Conflict and Interdependent Capabilities. This office has overall responsibility for the supervision of Special Operations (SO) and Low-intensity Conflict (LIC) activities of DoD - including oversight of policy and resources. The Cohen-Nunn Amendment to the DoD Authorization Act of 1987, established ASD(SO/LIC) and the United States Special Operations Command (USSOCOM). ASD(SO/LIC) is the principal civilian advisor to SECDEF on SO/LIC matters. The objectives of this amendment were:

- Provide close civilian oversight for special operations and low-intensity conflict activities.
- Ensure that genuine expertise and a diversity of views are available to the President and Secretary of Defense regarding possible responses to special operations requirements and low-intensity conflict threats.
- Is DoD lead for psychological operations (PSYOP) and coordination with USSOCOM.
- Improve interagency planning and coordination for special operations and low-intensity conflict.
- Bolster U.S. special operations capabilities in a number of areas to include joint doctrine and training, intelligence support, command and control, budgetary authority, personnel management, and mission planning.

The following offices fall under the ASD for Special Operations/Low Intensity Conflict and Interdependent Capabilities. :

- Office of the Deputy Assistant Secretary of Defense for Special Operations Capabilities
- Office of the Deputy Assistant Secretary of Defense for Strategic Capabilities
- Office of the Deputy Assistant Secretary of Defense for Forces Transformation & Resources
- Office of the Deputy Assistant Secretary of Defense for Stability Operations Capabilities

Website: <http://www.defenselink.mil/policy/>

Last Updated: October 2007

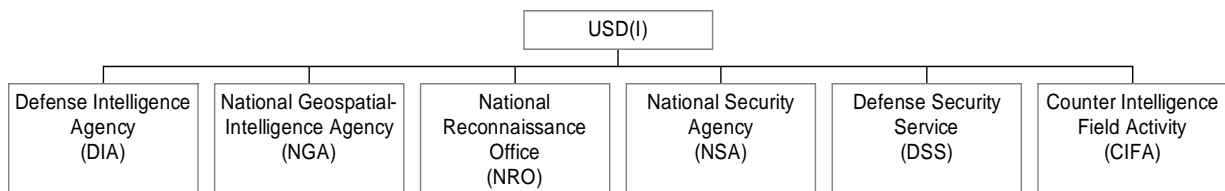
This Page Intentionally Blank

Under Secretary Of Defense for Intelligence (USD(I))



Mission

The Under Secretary of Defense for Intelligence (USD(I)) serves as the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense on all intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. The USD(I) also serves as the PSA to the Secretary of Defense on development and oversight of DoD IO policy and integration activities, and serves as the DoD lead with the Intelligence Community on DoD IO issues. Per a memorandum between the SecDef and the Director of National Intelligence (DNI) signed May 21, 2007, the USD(I) is also designated as the Director of Defense Intelligence (DDI) in the Office of the Director of National Intelligence. In this capacity, the USD(I) reports directly to the DNI and serves as the principal advisor to the DNI on defense intelligence matters.



Responsibilities:

Information Operations Responsibilities (extracted from DoDD 5143.01, 23 Nov 05):

- Serve as the Principal Staff Assistant to the Secretary of Defense for IO.
- Develop and oversee DoD IO policy and integration activities.
- Assess performance/responsiveness of DoD and Military Intelligence activities to support IO.
- Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements.
- Establish specific policies for the development and integration of CNO, MILDEC and OPSEC as core IO capabilities.

Other Responsibilities:

- Serve as the OSD proponent for the Information Operations Career Force (See DoDD 3608.11, “Information Operations Career Force”, 4 Nov 05).
- Providing oversight and policy guidance for all DoD intelligence activities and establishing priorities to ensure conformance with Secretary and, as appropriate, Director of National Intelligence (DNI) policy guidance.
- Exercise authority, direction, and control over the Defense Intelligence Agency (DIA), the National Geospatial Intelligence Agency (NGA), the National Reconnaissance Organization (NRO), the National Security Agency (NSA), the Defense Security Service (DSS), and the Counter Intelligence Field Activity (CIFA).
- Provide assessments of and advising the Secretary and the CJCS on the adequacy of military intelligence performance.
- Advise the Secretary concerning the Department's responsibilities regarding the national intelligence community and supporting the Secretary's role in the Intelligence Community Executive Committee.
- Exercise management and oversight of all DoD counterintelligence and security activities, including personnel security and industrial security.
- Oversee intelligence support to critical infrastructure protection, departmental information assurance programs and homeland defense.
- Coordinating DoD intelligence and intelligence-related policy, plans, programs, requirements and resource allocations. This includes responsibility for the DoD components within the National Foreign Intelligence Program, the Joint Military Intelligence Program, the Foreign Counterintelligence Program, and the Tactical Intelligence and Related Activities account.
- Ensuring the execution of DoD intelligence policy and resource decisions are fully responsive and complimentary to the direction of the DNI.
- Exercising overall supervision and policy oversight of the DoD intelligence infrastructure and civilian intelligence personnel management systems. This will include policy regarding the Defense Civilian Intelligence Personnel Systems (DCIPS).
- Maintain close coordination with the DNI and consult with the DNI on the development, design, acquisition and operation of intelligence programs and systems of the DOD.

Last Updated: September 2007

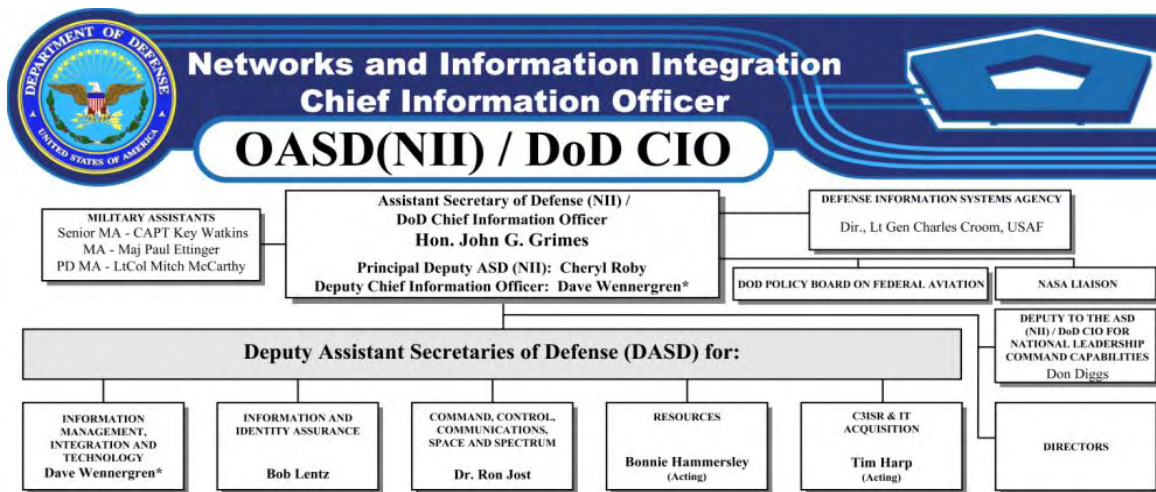
Assistant Secretary Of Defense – Networks And Information Integration (ASD(NII))



Mission and Goals.

The missions and responsibilities of the ASD(NII) are specified in Department of Defense Directive (DoDD) 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO)" dated 2 May 2005.

Organization:



The goals of ASD(NII) are to:

- Make information available on a network that people depend on and trust
- Populate the network with new, dynamic sources of information to defeat the enemy
- Deny the enemy information advantages and exploit weakness to support network centric warfare and the transformation of DoD business processes

Mission: The ASD(NII)/DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; Information Technology (IT), including National Security Systems (NSS); information resources management (IRM); spectrum management; network operations; information systems; information assurance (IA); positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters.

ASD(NII)/DoD CIO has responsibilities for integrating information and related activities and services across the Department. The ASD(NII)/DoD CIO also serves as the DoD Enterprise-level strategist and business advisor from the information, IT, and IRM perspective.

Responsibilities of the ASD(NII)/DoD CIO include the following:

- Information Operations: Provide NII and CIO support to the mission of Information Operations IAW DoD Directive S-3600.1.
- Information Assurance: Develop and maintain the DoD Information Assurance (IA) program and associated policies, procedures, and standards required by DoD Directive S-3600.1, “Information Operations”.
- Transformation: Develop and implement network-centric policies, architectures, practices, and processes with emphasis on communications and information networks to enable Defense transformation; however, these do not include content-based communications functions such as those associated with public affairs and public diplomacy.
- Global Information Grid: Facilitate and resolve interoperability, performance, and other issues related to interfaces, security, standards, and protocols critical to the end-to-end operation of the Global Information Grid (GIG).
- IT Opportunities: Identify opportunities presented by communication and information technologies as well as risks and costs, and make recommendations on the initiation of communication and information plans, programs, policies, and procedures accordingly.
- Electromagnetic Spectrum: Provide policy, oversight, and guidance for all DoD matters related to the electromagnetic spectrum, including the management and use of the electromagnetic spectrum (MUES) and the Electromagnetic Environmental Effects (E3) Program.
- Command and Control: Develop and integrate the Department’s overall C2 strategy, approach, structure, and policies and ensure the C2 structure and architecture are compliant with DoD network-centric precepts, information strategy, and joint needs.
- Space: Oversee DoD non-intelligence related space matters, including space-based communications programs, space-based information integration activities, space control activities, operationally responsive space programs, space access, satellite control, space-based position, navigation, and timing programs, environmental sensing, and space launch ranges.

Headquarters: The headquarters for the ASD(NII) organization is in the Pentagon, with staff elements both in the Pentagon and in nearby office buildings in Arlington, Virginia.

Website: <http://www.defenselink.mil/nii/>

Last Updated: October 2007

DoD Strategic Communication Integration Group (SCIG)



DOD published the “Quadrennial Defense Review (QDR) Execution Roadmap for Strategic Communication” in September 2006. The Roadmap outlined an action plan, setting responsibilities and milestones to improve DoD’s capability to support Strategic Communication (SC). The main objectives are to:

Institutionalize a DoD process to incorporate SC into strategy development, policy formulation, planning and execution.

Define roles, responsibilities and relationships, and develop doctrine for SC.

Properly resource Military Departments and Combatant Commands to organize, train, and equip DoD’s primary communication supporting capabilities.

DoD Strategic Communication Integration Group Charter

Objectives

The SCIG is a forum for the overarching review of DoD SC activities, and consists of senior representatives from OSD, the Joint Staff, the Combatant Commands and the Military Departments, as designated by those respective organizations. Other DoD organizations and representatives of other US Government departments and agencies will be invited by the SCIG EXCOM as appropriate. Members of the SCIG will be provided information on the SC priorities and activities of the Department and the SCIG EXCOM on at least a semi-annual basis. Additionally, members of the SCIG will appoint SC directors, generally at the 2-star to colonel level or civilian equivalent to represent them. The SC Directors’ Group is intended to serve as a means for the day-to-day coordination of SC throughout OSD, the Joint Staff, the Combatant Commands and Military Departments.

The development, coordination, approval, and implementation of formally detailed SC plans will normally be assigned to a particular command or component, with review by the Joint Staff and OSD, as with other plans. Broad strategic guidance for development of these plans will be issued through the SCIG process, as will any approvals for taskings and resources. By exception, plans that are global in their primary character may be assigned for lead to the Joint Staff or OSD, if not assigned to a command. Detailed coordination across the Department, with other US Government agencies, and with coalition partners will be the responsibility of the assigned lead, although OSD, the Joint Staff, and the SCIG Secretariat will assist where necessary. OSD (Policy) remains the principal lead for formal policy coordination on SC guidance and plans with other U.S. Government departments and agencies. ASD(PA) remains the lead for formal coordination on issues of public communication with other U.S. Government departments and agencies.

The SCIG EXCOM consists of the Assistant Secretary of Defense (Public Affairs) (ASD(PA)), the Principal Deputy Under Secretary of Defense (Policy), and the Director of the Joint Staff. Others who participate on an ex-officio basis will normally include ASD(LA), OSD(GC), and key members of the Joint Staff. The SCIG EXCOM will meet regularly (at least twice a month) to assess and synchronize SC activities, programs, actions and information of importance, and will recommend proposed strategic guidance for my approval.

Definition of Strategic Communication: *Focused U.S. Government (USG) processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power.*

SCIG will play a central role in facilitating coordination within and among DoD organizations and USG agencies to integrate strategic communications into U.S. national security policy, planning, and execution. It will address two categories of issues: long-range trends and objectives of broad scope and importance; and emergent issues of interest and immediate significance that need coordination across several agencies.

The DoD primary communication supporting capabilities that support the strategic communication process are public affairs (PA), visual information (VI), defense support to public diplomacy (DSPD), and military information operations (IO) - principally Psychological Operations (PSYOP). The SCIG will work to ensure synchronization and horizontal integration of plans and efforts among these communication disciplines and across the department.

SCIG Functions

- Advise the Secretary and Deputy Secretary of Defense and the Chairman of the Joint Chiefs of Staff in setting strategic communication goals and priorities and on issuing guidance to appropriate DoD audiences;
- Integrate DoD and USG strategic communications strategies, plans, and programs within and among appropriate DoD and interagency organizations;
- Identify policies, issues, programs, and operations that may have strategic communication implications and advise the Secretary of Defense, the Deputy Secretary of Defense, and the Chairman of the Joint Chiefs of Staff on how to address them;
- Review and generate recommendations on strategic-level proposals developed by DoD or other USG organizations for the Secretary and Deputy Secretary of Defense and Chairman of the Joint Chiefs of Staff; and
- Inform the Secretary, the Deputy Secretary of Defense and the Chairman of the Joint Chiefs of Staff on the impact of DoD and U.S. Government strategic communication efforts.

Membership

Primary members and co-chairs are USD(P), ASD(PA), Director, Joint Staff.

Associate members will be provided topics and briefings proposed for the SCIG and will be invited to attend meetings at the SCIG's discretion. Associate members include:

USD(I)
USD(AT&L)
USD(P&R)
USD(C)
ASD(NII)
Director, PA&E
ACJCS
Director, Joint Staff J2
Director, Joint Staff J3
Director, Joint Staff J5

OCJCS Public Affairs
OCJCS Legislative Affairs
OCJCS Legal Counsel
US Army
US Navy
US Air Force
US Marine Corps
SOCOM
STRATCOM
JFCOM

Other DoD or interagency organizations may be invited to participate in briefings when the particular topic is appropriate to their area of responsibility.

DoD SCIG Secretariat

The SCIG Secretariat is tasked to ensure SC products from OSD, the Joint Staff, the Combatant Commanders, and the Military Departments are coordinated and synchronized across the Department and the rest of the US Government. The SCIG Secretariat will also perform SC-related staff work to support the EXCOM and the Department, including issue identification, preparation of SC guidance, the development of SC processes and initiatives, and linking information and communication issues with broader policies, plans and actions.

The Director of the SCIG Secretariat will be approved by the Deputy Secretary. The Director will routinely inform and advise SCIG Principals on the work of the Secretariat.

The DoD SCIG Secretariat consists of full-time representatives from OSD and the Joint Staff. The members will be O-5/O-6 level or civilian equivalent. Their principal task will be to serve in the DoD SCIG Secretariat. Members will stay engaged at the senior levels with appropriate organizations, for example attending senior staff meetings and briefings of strategic-level issues

SCIG Secretariat Members will be provided from the following components:

SD(P)
USD(I)
USD(P&R)
USD(AT&L)
ASD(LA)
ASD(PA)
Joint Staff

Last Updated: November 2007.

This Page Intentionally Blank

Defense Information Systems Agency (DISA)



Mission:

DISA is the premier provider of current and future command and control (C2) and combat support capabilities that support the joint warfighter with planning and executing joint military and coalition operations. The director of DISA also serves as the commander, Joint Task Force-Global Network Operations (JTF-GNO), a subordinate organization to USSTRATCOM.

History of DISA

The Defense Information Systems Agency (DISA) was established as the Defense Communications Agency (DCA) in 1960. Its mission was to manage the Defense Communications System (DCS), a consolidation of the independent long-haul communications functions of the Army, Navy, and Air Force. Later, took on several major organizations, to include the White House Signal Agency (now the White House Communications Agency). DCA also established six regional communications control centers and two area centers for operational control of the DCS. DCA later became responsible for engineering and operating the Worldwide Military Command and Control System.

In the 1980s, DCA absorbed the Joint Tactical Command, Control, and Communications Agency and was renamed DISA in 1991. DCA implemented creation of the Defense Information Infrastructure, now known as the Global Information Grid (GIG). DISA consolidated several information processing centers into five mainframe-processing centers. The Joint Spectrum Center and the Defense Technical Information Center also became part of DISA. Approximately 7,000 military and civilian employees work in DISA.

Operations and Activities:

DISA's current C2 programs include the Global Command and Control System – Joint (GCCS-J), Global Combat Support System for the Combatant Command and Joint Task Force (GCSS CC/JTF), and the future C2 system of record, the Net-Enabled Command Capability (NECC), formerly known as the Joint Command and Control (JC2) Capability. Through NECC, DISA will direct the evolution of the current C2 programs to deliver a truly integrated, joint, net-centric C2 capability for the warfighter. DISA also has various Advanced Concept Technology Demonstrations (ACTDs) and Joint Capability Technology Demonstrations (JCTDs) that facilitate rapid development of advanced capabilities.

Through GCCS-J, DISA enables Joint operations planning and execution, global access to mandated readiness data, situational awareness via a common operational picture, Commander's understanding of the battlespace through imbedded/integrated intelligence and imagery products, and collaboration and decision support capabilities for Combatant Commanders and Joint Force Commanders. Deployed worldwide, GCCS-J components form the critical C2 backbone of Joint operations. Lighter, configurable deployments of GCCS-J support selected Joint Task Forces and Coalition operations. GCCS-J

intelligence products and training are currently being used in direct support of OEF, OIF, and NATO/ISAF Afghanistan Operations. In addition, GCCS-J has successfully supported such non-traditional missions as investigation as a capability that could be used to deal with a potential Avian Flu pandemic. GCCS-J is in the midst of its Block V development and fielding phase, which will provide even more substantial C2 capabilities to the Warfighter, including many technological solutions that exploit the emerging availability of the Service Oriented Architecture.

DISA provides the logistics C2 system of record through GCSS CC/JTF. GCSS CC/JTF is an integration and interoperability initiative to better meet the operational needs of the warfighter for combat support. As part of its mission, GCSS CC/JTF enhances combat support effectiveness through system interoperability across combat support and combat service support functions, and between combat support and command and control functions. GCSS CC/JTF expands the availability, accuracy, and timeliness of information to the combatant commanders and the joint task force commanders and their staffs through information fusion. End-users have the ability to create a user defined operational picture through dynamic access to disparate data sources and enhanced by a tool kit of capabilities such as knowledge management, business intelligence, watchboard, electronic battlebook, functional applications and access to other SIPRNet sites via one GCSS gateway.

As the ASD(NII) designated NECC Lead Component, DISA, in concert with the joint community, will revolutionize DoD C2. NECC will become DoD's principal command and control capability that will be accessible in a net-centric environment. It will be founded on a single, net-centric, services-based C2 architecture and will provide the decision support infrastructure that will enable the warfighter to access, display, and understand the information necessary to make efficient, timely, and effective decisions. Today's C2 capabilities that support the warfighter are aligned with functions, resulting in separate stovepipes. This limits flexibility needed across the C2 environment, and places the burden on the warfighter to pull and gather the disparate information required to perform C2 functions. The warfighter is forced to serve as the C2 Information Integrator. NECC will replace the current C2 stovepiped capabilities by creating C2 capabilities that provide access to information from a multitude of sources. This will allow the ability to merge all types of information to develop pictures, ideas, and understandings the warfighter has never had before. NECC will also provide a dynamic C2 capabilities construct where the user can define the functions or C2 capabilities needed and clearly define the mission threads. Warfighters will be able to rapidly adapt to changing mission needs by defining and tailoring their information environment and drawing on capabilities that enable the efficient, timely, and effective command of forces and control of engagements. By changing the focus from stovepiped capabilities to data, the warfighter gains an extremely dynamic and integrated information environment.

DISA is deeply involved in ACTDs, working with the Combatant Commanders to pilot key capabilities essential to the Department's ongoing transformation. ACTDs respond to high-priority capability shortfalls involving complex conceptual or technical issues appropriately addressed early in a technology lifecycle. ACTDs are typically three to five years in duration and usually transition into a Program of Record upon successful completion. While that is fairly rapid in terms of capability deployment, it isn't fast enough in today's world. Our ops tempo requires even more rapid deployment. JCTDs are typically 18 months to three years in duration and are funded with a higher percentage of OSD AS&C money. JCTDs, like ACTDs, usually transition upon successful completion into a Program of Record. This gives Combatant Commanders yet another means of rapidly addressing immediate operational needs.

As of 29 Aug 06, DISA's active ACTD and JCTDs include:

- Agile Transportation 21st Century including Turbo Planner – AT21
- Event Management Framework - EMF
- Coalition Secure Management and Operations Systems - COSMOS
- Joint Coordinated Real-time Engagement - JCRE
- Coalition Theater Logistics - CTL

- Joint Force Projection – JFP
- GRIDLOCK
- Theater Effects Based Operations - TEBO
- Homeland Security C2 – HLS C2
- Large Data JCTD
- Actionable Situational Awareness Picture - ASAP
- Medical Situational Awareness In-Theater – MSAT

Website: <http://www.disa.mil>

Last Updated: September 2007

This Page Intentionally Blank

Information Assurance Technology Analysis Center (IATAC)



The Information Assurance Technology Analysis Center (IATAC) is a U.S. Department of Defense Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC), and Director, Defense Research & Engineering (DDR&E). [see internet site: <http://www.dod.mil/ddre/>.]

Mission:

Provide the DoD a central point of access for information on Information Assurance (IA) emerging technologies in system vulnerabilities, research and development, models, and analysis to support the development and implementation of effective defense against Information Warfare attacks.

Management and Direction of IATAC Operations:

IATAC operates under the direction of our Government Steering Committee. The committee is made up of 19 individuals from Government, DoD and the research and development (R&D) community, including representation from the Defense Information Assurance Program (DIAP), Joint Task Force for Global Network Operations (JTF-GNO), National Security Agency (NSA), Naval Postgraduate School (NPS), Office of the Secretary of Defense (OSD), and the Navy Information Operations Command - Norfolk, to name a few. The steering committee meets once a year and provides input and feedback to IATAC's operations, particularly our information collection and information dissemination efforts. Additionally, the topics of the technical reports that IATAC authors are dictated by our Steering Committee.

History:

The United States is vulnerable to Information Warfare attacks because our economic, social, military, and commercial infrastructures demand timely and accurate as well as reliable information services. This vulnerability is complicated by the dependence of our DoD information systems on commercial or proprietary networks which are readily accessed by both users and adversaries. The identification of the critical paths and key vulnerabilities within the information infrastructure is an enormous task. Recent advances in information technology have made information systems easier to use, less expensive, and more available to a wide spectrum of potential adversaries.

Our nation's information infrastructure depends on the survivability, authenticity, and continuity of DoD information systems. These systems are vulnerable to external attacks, due in part to the necessary dependence on commercial systems and the increased use of the Internet. The survivability, authenticity, and continuity of DoD information systems is of supreme importance to the Warfighter. With the increasing amount of concern and Information Warfare activities requiring rapid responses, it is difficult to ensure that all appropriate agencies and organizations are given the knowledge and tools to protect from, react to, and defend against Information Warfare attacks. IATAC was established under the direction of DTIC and the integrated sponsorship of the Defense Information Systems Agency (DISA); the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII); the Joint Staff (J6); and DDR&E, whose missions direct the DoD's responses, developments, and operations regarding IA.

IATAC provides a central authoritative source for IA vulnerability data, information, methodologies, models, and analyses of emerging technologies relating to the survivability, authenticity, and continuity of operation of information systems critical to the nation's defense in support of the Warfighter's front line missions. IATAC's support extends across the spectrum from policy, doctrine, and strategy development, to R&D, S&T, engineering, and architecture, to operations and training. This spectrum of activities ensures the collection, analysis, and dissemination of a broad and growing library of scientific technical information (STI) related to IA. IATAC serves to help synchronize DoD's IA efforts across that entire spectrum of activities as well as into the civil/federal government.

IATAC operates as a specialized subject focal point, supplementing DTIC services within DoD Directive 3200.12, DoD Scientific and Technical Information Program (STIP), dated 15 February 1983.

Location and Contact Information:

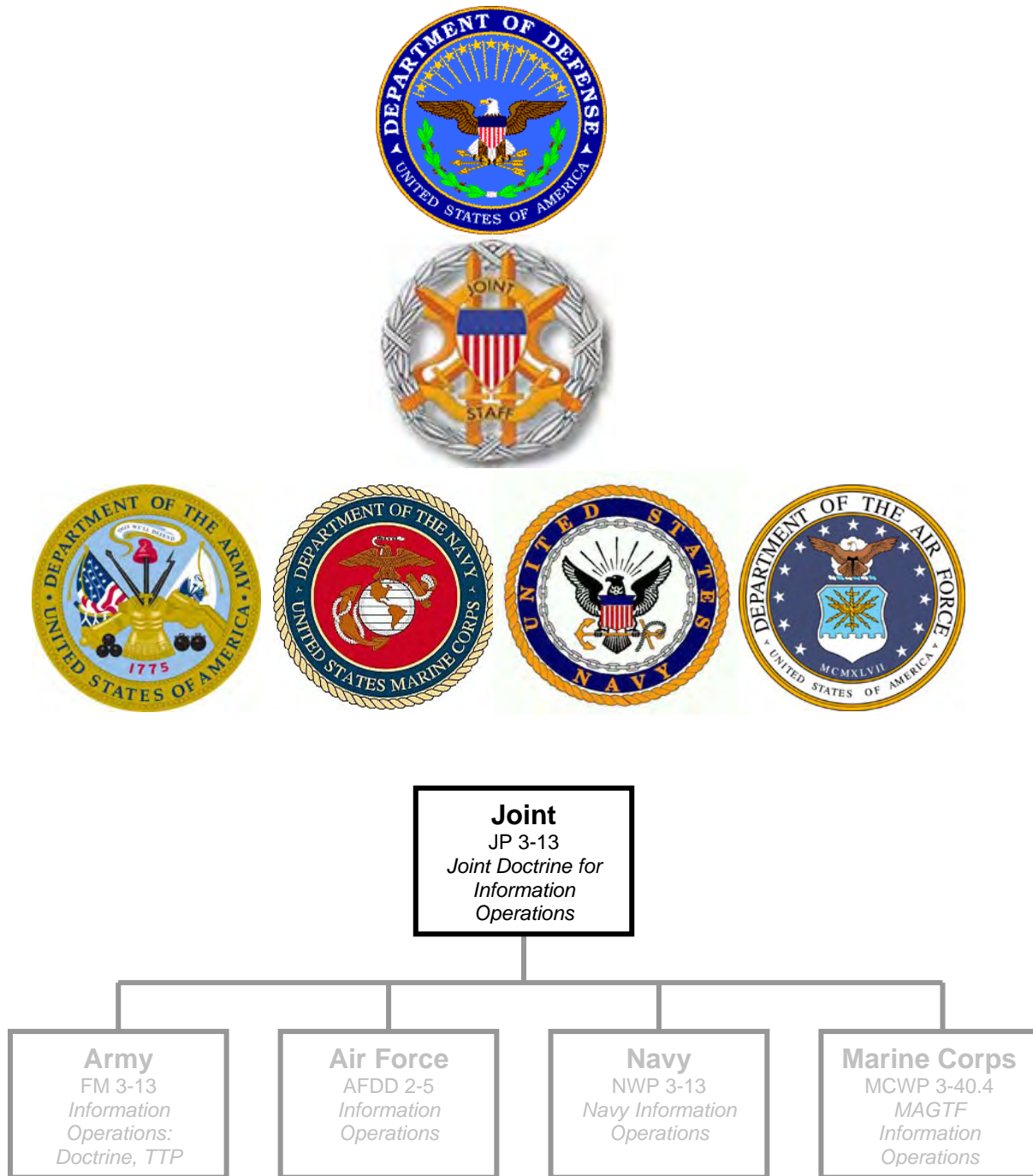
IATAC

13200 Woodland Park Road
Herndon, VA 20171
Phone: (703) 984.0775
Fax: (703) 984.0773
E-mail: iatac@dtic.mil

Website: iac.dtic.mil/iatac/

Last updated: October 2007

Joint Information Operations Doctrine and Vision



This Page Intentionally Blank

Joint Information Operations Doctrine



Key doctrinal documents:

Joint Pub 3-13, *Information Operations*, 13 February 2006
Joint Pub 3-13.1, *Electronic Warfare*, 25 January 2007
Joint Pub 3-13.3, *Operations Security*, 29 June 2006
Joint Pub 3-13.4, *Military Deception*, 13 July 2006
Joint Pub 3-53, *Doctrine for Joint Psychological Operations*, 5 September 2003
Joint Pub 3-57, *Joint Doctrine for Civil-Military Operations*, 8 February 2001
Joint Pub 3-61, *Public Affairs*, 9 May 2005

Joint Pubs available at: http://www.dtic.mil/doctrine/s_index.html and at
<https://jdeis.js.mil/jdeis/index.jsp>.

Joint Information Operations doctrine is set down in Joint Publication 3-13. This section extracts the publication's executive summary, below.

EXECUTIVE SUMMARY, JOINT PUBLICATION 3- 13

- **Discusses the Information Environment and Its Relationship to Military Operations**
- **Discusses the Information Operations (IO) Core Capabilities Necessary to Successfully Plan and Execute IO to include Supporting and Related Capabilities in a Joint/Multinational Environment**
- **Aligns Joint IO Doctrine with the Transformational Planning Guidance as Specified by the Department of Defense IO Roadmap for Achieving Information Superiority on the Battlefield**
- **Provides an Organizational Framework for Integrating, Deconflicting, and Synchronizing IO Planning and Execution Activities for Supporting and Supported Combatant Command Staffs, National Intelligence Agencies, and Other Federal Agencies as Applicable**
- **Outlines Planning Considerations for Developing an IO Career Force through Joint Education, Training, Exercises, and Experimentation**

Military Operations and the Information Environment

To succeed, it is necessary for US forces to gain and maintain information superiority.

Information is a strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities.

Information operations (IO) are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

The purpose of this doctrine is to provide joint force commanders (JFCs) and their staffs guidance to help prepare, plan, execute, and assess IO in support of joint operations. The principal goal is to achieve and maintain information superiority for the US and its allies.

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.

Core, Supporting, and Related Information Operations Capabilities

Core capabilities.

IO consists of five core capabilities which are: PSYOP, MILDEC, OPSEC, EW, and CNO. Of the five, PSYOP, OPSEC, and MILDEC have played a major part in military operations for many centuries. In this modern age, they have been joined first by EW and most recently by CNO. Together these five capabilities, used in conjunction with supporting and related capabilities, provide the JFC with the principal means of influencing an adversary and other target audiences (TAs) by enabling the joint forces freedom of operation in the information environment.

Supporting capabilities.

Capabilities supporting IO include information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. These are either directly or indirectly involved in the information environment and contribute to effective IO. They should be integrated and coordinated with the core capabilities, but can also serve other wider purposes.

Related capabilities.

There are three military functions, public affairs (PA), civil military operations (CMO), and defense support to public diplomacy, specified as **related capabilities for IO**. These capabilities make significant contributions to IO and must always be coordinated and integrated with the core and supporting Information Operations capabilities. However, their primary purpose and rules under which they operate must not be compromised by IO. This requires additional care and consideration in the planning and conduct of IO. For this reason, the PA and CMO staffs particularly must work in close coordination with the IO planning staff.

Intelligence and Communications System Support to Information Operations

Successful planning, preparation, execution, and assessment of information operations (IO) demand detailed and timely intelligence.

Before military activities in the information environment can be planned, the current “state” of the dynamic information environment must be collected, analyzed, and provided to commanders and their staffs. This requires intelligence on relevant portions of the physical, informational, and cognitive properties of the information environment, which necessitates collection and analysis of a wide variety of information and the production of a wide variety of intelligence products.

Nature of IO intelligence requirements.

In order to understand the adversary or other TA decision-making process and determine the appropriate capabilities necessary to achieve operational objectives, commanders and their staffs must have current data. This includes relevant physical, informational, and cognitive properties of the information environment as well as assessment of ongoing IO activities.

Intelligence considerations in planning IO.

Intelligence Resources are Limited. Commanders and their intelligence and operations directorates must work together to identify IO intelligence requirements and ensure that they are given high enough priority in the commander’s requests to the intelligence community (IC).

Collection Activities are Legally Constrained. The IC must implement technical and procedural methods to ensure compliance with the law. Additionally, intelligence may be supplemented with information legally provided by law enforcement or other sources.

Intelligence Support to IO Often Requires Long Lead Times. The intelligence necessary to affect adversary or other TA decisions often requires that specific sources and methods be positioned and employed over time to collect the necessary information and conduct the required analyses.

Information Environment is Dynamic. Commanders and their staffs must understand both the timeliness of the intelligence they receive and the differing potentials for change in the dimensions of the information environment.

Properties of the Information Environment Affect Intelligence. Collection of physical and electronic information is objectively measurable by location and quantity. Commanders and their staffs must have an appreciation for the subjective nature of psychological profiles and human nature.

Responsibilities and Command Relationships

Joint Staff.

The Chairman’s responsibilities for IO are both general (such as those to establish doctrine, provide advice, and make recommendations) and specific (such as those assigned in DOD IO policy). The Operations Directorate of the Joint Staff (J-3) serves as the Chairman’s focal point for IO and coordinates with the other organizations within the Joint Staff that have direct or supporting IO responsibilities. The IO divisions of the Joint Staff J-3 provide IO specific advice and advocate Joint Staff and combatant commands’ IO interests and concerns within DOD and interact with other organizations and individuals on behalf of the Chairman.

- Combatant commands.*** Commander, United States Strategic Command's (USSTRATCOM's) specific authority and responsibility to coordinate IO across area of responsibility (AOR) and functional boundaries does not diminish **the imperative for other combatant commanders to employ IO**. These efforts may be directed at achieving national or military objectives incorporated in theater security cooperation plans, shaping the operational environment for potential employment during periods of heightened tensions, or in support of specific military operations. It is entirely possible that in a given theater, the combatant commander will be supported for select IO while concurrently supporting USSTRATCOM IO activities across multiple theater boundaries.
- Components.*** **Components** are normally responsible for detailed planning and execution of IO. IO planned and conducted by functional components must be conducted within the parameters established by the JFC. At the same time, component commanders and their subordinates must be provided sufficient flexibility and authority to respond to local variations in the information environment. Component commanders determine how their staffs are organized for IO, and normally designate personnel to liaise between the JFC's headquarters and component headquarter staffs.
- Subordinate joint force commanders.*** Subordinate JFCs plan and execute IO as an integrated part of joint operations. Subordinate staffs normally share the same type of relationship with the parent joint force IO staff as the Service and functional components. **Subordinate JFC staffs may become involved in IO planning and execution to a significant degree**, to include making recommendations for employment of specific capabilities, particularly if most of the capability needed for a certain operation resides in that subordinate joint task force.
- Organizing for joint IO.*** Combatant commanders normally **assign responsibility for Information Operations** to the J-3. When authorized, the director of the J-3 has primary staff responsibility for planning, coordinating, integrating, and assessing joint force IO. **The J-3 normally designates an Information Operations cell chief** to assist in executing joint IO responsibilities. The primary function of the IO cell chief is to ensure that IO are integrated and synchronized in all planning processes of the combatant command staff and that IO aspects of such processes are coordinated with higher, adjacent, subordinate, and multinational staffs. To integrate and synchronize the core capabilities of IO with IO-supporting and related capabilities and appropriate staff functions, the IO cell chief normally leads an "IO cell" or similarly named group as an integrated part of the staff's operational planning group or equivalent. The organizational relationships between the joint IO cell and the organizations that support the IO cell are per JFC guidance.

Planning and Coordination

- IO planning follows the same principles and processes established for joint operation planning.*** The IO staff coordinates and synchronizes capabilities to accomplish JFC objectives. Uncoordinated IO can compromise, complicate, negate, or harm other JFC military operations, as well as other USG information activities. JFCs must ensure Information Operations planners are fully integrated into the planning and targeting process, assigning them to the joint targeting coordination board in order to ensure full integration with all other planning and execution efforts. Other USG and/or coalition/allied information activities, when uncoordinated, may complicate, defeat, or render DOD IO

ineffective. Successful execution of an information strategy also requires early detailed JFC IO staff planning, coordination, and deconfliction with USG interagency efforts in the AOR to effectively synergize and integrate IO capabilities.

Planning considerations. IO planning must begin at the **earliest stage** of a JFC's campaign or operations planning and must be an integral part of, not an addition to, the overall planning effort. IO are used in all phases of a campaign or operation. The use of IO during early phases can significantly influence the amount of effort required for the remaining phases.

The use of IO in peacetime to achieve JFC objectives and to preclude other conflicts, requires an ability to integrate Information Operations capabilities into a comprehensive and coherent strategy through the establishment of information objectives that in turn are integrated into and support the JFC's overall mission objectives. The combatant commander's theater security cooperation plan serves as an excellent platform to embed specific long-term information objectives

IO planning requires early and detailed preparation. Many Information Operations capabilities require long lead-time intelligence preparation of the battlespace (IPB). IO support for IPB development differs from traditional requirements in that it may require greater lead time and may have expanded collection, production, and dissemination requirements. Consequently, combatant commanders must ensure that IO objectives are appropriately prioritized in their priority intelligence requirements (PIRs) and requests for information (RFIs).

As part of the planning process, designation of release and execution authority is required. Release authority provides the approval for IO employment and normally specifies the allocation of specific offensive means and capabilities provided to the execution authority. Execution authority is described as the authority to employ IO capabilities at a designated time and/or place. Normally, the JFC is the one execution authority designated in the execute order for an operation.

IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval.

Commander's intent and information operations. The commander's vision of IO's role in an operation should begin before the specific planning is initiated. A commander that expects to rely on IO capabilities must ensure that IO related PIRs and RFIs are given high enough priority prior to a crisis, in order for the intelligence products to be ready in time to support operations. At a minimum, the commander's vision for IO should be included in the initial guidance. Ideally, commanders give guidance on Information Operations as part of their overall concept, but may elect to provide it separately.

Measures of performance and measures of effectiveness. **Measures of performance (MOPs)** gauge accomplishment of Information Operations tasks and actions. **Measures of effectiveness (MOEs)** determine whether IO actions being executed are having the desired effect toward mission accomplishment: the attainment of end states and objectives. MOPs measure friendly IO effort and MOEs measure battlespace results. IO MOPs and MOEs are crafted and refined throughout the planning process.

Multinational Considerations in Information Operations

Every ally/coalition member can contribute to IO by providing regional expertise to assist in planning and conducting IO.

Allies and coalition partners recognize various IO concepts and some have thorough and sophisticated doctrine, procedures, and capabilities for planning and conducting IO. **The multinational force commander is responsible to resolve potential conflicts** between each nation's IO programs and the IO objectives and programs of the coalition. It is vital to integrate allies and coalition partners into IO planning as early as possible so that an integrated and achievable IO strategy can be developed early in the planning process.

Integration requirements include clarification of allied and coalition partner's IO objectives; understanding of other nations' information operations and how they intend to conduct IO; establishment of liaison/deconfliction procedures to ensure coherence; and early identification of multinational force vulnerabilities and possible countermeasures to adversary attempts to exploit them.

Information Operations in Joint Education, Training, Exercises, and Experiments

A solid foundation of education and training is essential to the development of IO core competencies.

The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities at all levels of DOD. At the highest professional levels, senior leaders develop joint warfighting core competencies that are the capstone to American military power. The Services, United States Special Operations Command, and other agencies develop capabilities oriented on their core competencies embodied in law, policy, and lessons learned. At each level of command, a solid foundation of education and training is essential to the development of a core competency. Professional education and training, in turn, are dependent on the accumulation, documentation, and validation of experience gained in operations, exercises, and experimentation.

IO education considerations.

The IO career force should consist of both capability specialists (EW, PSYOP, CNO, MILDEC, and OPSEC) and IO planners. Both groups require an understanding of the information environment, the role of IO in military affairs, how IO differs from other information functions that contribute to information superiority, and specific knowledge of each of the core capabilities to ensure integration of IO into joint operations.

IO planners are required at both the component and the joint level.

Senior military and civilian DOD leaders require an executive level knowledge of the information environment and the role of IO in supporting DOD missions.

IO training considerations.

Joint military training is based on joint policies and doctrine to prepare joint forces and/or joint staffs to respond to strategic and operational requirements deemed necessary by combatant commanders to execute their assigned missions.

IO training must support the IO career force and be consistent with the

joint assignment process. Joint IO training focuses on joint planning-specific skills, methodologies and tools, and assumes a solid foundation of Service-level IO training.

The Services determine applicable career training requirements for both their IO career personnel and general military populations, based on identified joint force mission requirements.

CONCLUSION

This document [JP 3-13] provides the doctrinal principles for DOD employment of IO. It has been designed to provide overarching guidance in the planning and execution of IO in today's joint/ multinational security environment. Its primary purpose is to ensure all of the capabilities comprising IO are effectively coordinated and integrated into our nation's warfighting capability against current and future threats.

Updated: November 2007

This Page Intentionally Blank

Joint Vision 2020 and Information Superiority



Purpose. The Department of Defense issued “Joint Vision 2020” (JV2020) in May, 2000 to update the conceptual “template” that guides the transformation of the U.S. Armed Forces into a 21st Century force. The document replaced the July 1996 “Joint Vision 2010”.

Although JV2020 is, at this printing of the Primer, seven years old, it still sets out the broad goals and the context for the on-going DoD force transformation process at large. It must be admitted that there is some debate as to how long former Defense Secretary Rumsfeld’s transformation objectives will survive his departure.

Goal. JV2020 depicted a “transformed” Force that would be, “dominant across the full spectrum of military operations – persuasive in peace, decisive in war, preeminent in any form of conflict”. Transformation efforts must go beyond technology and embrace doctrine, training, organization, education and leadership.

The document outlined what it anticipated would be the future security environment, described “full spectrum dominance”, and then discussed the key importance of information and technical innovation. Efforts to transform the force, it stated, depended upon, “realizing the potential of the information revolution”, which would change the very way that military operations take place. This revolution is creating both a quantitative as well as a qualitative change in the nature of information. Further, the pace of that change continues to accelerate.

The Strategic Context. JV2020 outlined three aspects of the global security environment confronting the U.S. and its friends in the 21st Century.

- First, the U.S. would continue to become more involved in an increasingly global economy, leading to greater interaction with a variety of regional entities.
- Second, potential adversaries will be able to access much of the technology and commercial commodities available to U.S. forces, to include information.
- Third, potential adversaries will adapt “niche” capabilities in the face of U.S. technological advantages that will enable them to target American capabilities where the disparity of strength is not as great, or adopt “asymmetric approaches”.

Information. The nature of information, its processing and its sharing is fundamental to all military operations and the information revolution presents the Force challenges and opportunities. Information and information technology are key to successful transformation efforts.

“Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions. The joint force must be able to

take advantage of superior information converted to superior knowledge to achieve “decision superiority” – better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. Decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary.

“The evolution of information technology will increasingly permit us to integrate the traditional forms of information operations with sophisticated all-source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign. The development of a concept labeled the global information grid will provide the network-centric environment required to achieve this goal. The grid will be the globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel. It will enhance combat power and contribute to the success of non-combat military operations as well. Realization of the full potential of these changes requires not only technological improvements, but the continued evolution of organizations and doctrine and the development of relevant training to sustain a comparative advantage in the information environment.”

In a concluding section JV2020 looks at the nature of technological innovation and also describes the increasing need for joint and combined operations capabilities, to include interagency cooperation. It broadly discusses precision engagement, focused logistics, joint command and control, and the role of information operations in achieving “full spectrum dominance”.

Complete JV2020 (Jun 2000) is available at: <http://www.dtic.mil/jointvision/jvpub2.htm>

Updated: October 2007

Joint Organizations and Educational Institutions



This Page Intentionally Blank

Joint Staff, Deputy Director for Global Operations (DDGO)



Mission:

The Deputy Director for Global Operations (DDGO) is responsible to the Director for Operations and the Chairman of the Joint Chiefs of Staff for providing expertise and advice in coordinating joint global operations to include information operations. Within the DDGO, the Assistant Deputy Director for Information Operations (DDGO/IO) is responsible for IO activities, developing joint IO policy and doctrine, and coordinating with the Office of the Secretary of Defense, combatant commands, Services, Defense Agencies, other staff directorates, the Intelligence Community, and interagency on IO issues/actions. In addition, the DDGO/IO is the focal point for all special technical operations.

Organization:

The Directorate for Global Operations contains four divisions:

The **Information Operations Division (IOD)** facilitates and coordinates electronic warfare (EW), computer network operations (CNO), special capabilities and Strategic Communication for the Chairman and in support of all Combatant Commands (COCOM) with the Office of the Secretary of Defense (OSD) and select interagency partners. Some of the tasks performed by IOD are:

- Support to COCOM requirements in EW, CNO, and Special Technical Operations (STO)
- Advocate IO related COCOM issues to the interagency
- Provide COCOMs with Science & Technology support for COA development

IOD consists of the following branches: Combatant Command Support, Plans Support, Computer Network Attack/Defense, Electronic Warfare, Intelligence Community Liaisons, Science and Technology, and Strategic Multi-layer Analysis Management.

The **Psychological Operations Division (POD)** develops and provides guidance to, and coordinates with, COCOMs and Services to plan and conduct Psychological Operations (PSYOP). Some of the tasks performed by POD are:

- Prepare, staff and transmit PSYOP specific execute orders, deployment orders, and PSYOP program approval
- Coordinate PSYOP activities with other US Government agencies
- Coordinate present and future manning & equipment issues

POD is composed of the Programs & Doctrine and the Combatant Command Support branches.

The **Program Support Division (PSD)** provides operational capabilities to the Joint Staff and COCOMs enabling warfighters, while building the foundation for an educated and trained cadre of IO Warriors. As part of this mission, PSD is the Joint Staff focal point for STO programmatics, policies and procedures, and is responsible for Joint IO policy and doctrine coordination and Joint IO Career Force Oversight. Some of the tasks performed by PSD are:

- Develop and coordinate STO policies & procedures
- Develop and coordinate joint IO policy & doctrine
- Oversight of the Joint IO Career Force
- Provide global network & 24/7 Planning and Decision Aid System (PDAS) support

PSD consists of the following branches: Policy & Doctrine, Programs, Automated Information Systems/Budget, Network Support, and the PDAS Support Center.

The **Special Actions Division (SAD)** develops and promulgates Joint policy and serves as the COCOMs' operational link to CJCS, SecDef and select interagency partners for Military Deception (MILDEC), Operations Security (OPSEC) and Defense Sensitive Support Activities. Some of the tasks performed by SAD are:

- Develop and coordinate MILDEC security policy
- Develop and coordinate OPSEC and MILDEC joint doctrine publications
- Serve as the Joint Staff focal point office for the Defense Sensitive Support Program
- Coordinate all Defense Sensitive Support requirements between OSD and other Government agencies with the Services and Combatant Commanders

SAD is composed of the Support Activities Branch and the Tactical Security Branch.

Location:

The DDGO is located within the Pentagon.

Website: <http://www.dtic.mil/jcs/>

Last Updated: September 2007

Joint Spectrum Center (JSC)



Mission: To enable effective and efficient use of the electromagnetic spectrum and control of electromagnetic effects in support of national security and military objectives.

Major Responsibilities

- Provides operational spectrum management support to the Joint Staff and COCOMs for contingency operations, exercises, and otherwise as requested.
- Conducts research and development (R&D) into spectrum efficient technologies to improve the Department's use of spectrum.
- Facilitates global spectrum information exchange by developing protocols, standards, applications, and information systems.
- Implements the DoD Joint Electromagnetic Environmental Effects (E3) Program.
- Develops, maintains, and distributes spectrum engineering and E3 analysis models, simulations, software, and data.
- Develops, distributes, and conducts E3 and spectrum management training courses for DoD Components.
- Provides technical E3 and spectrum engineering support, on a customer funded basis, to DoD, Federal Government organizations, the private sector when it is in the interest of national defense, and to foreign entities when authorized

The major functional components of JSC include the following:

J3 Operations Division. -- provides Communications-Electronics (C-E)/Electromagnetic Battlespace (EMB) support and Joint Spectrum Interference Resolution (JSIR) support to the Joint Staff, Unified Combatant Commands, and warfighting commanders. This support is available for both contingencies and joint training exercises and can be provided from the JSC or on-site.

J5 Research Development and Acquisition Division. -- manages the Joint DoD E3 Program. The primary goal of this program is to ensure that weapon systems and other equipment provided to our Warfighters are electromagnetically compatible with the battlefield electromagnetic EM environment and are supportable in the Electromagnetic Spectrum (EMS). The major divisions of the E3 program are: Milestone Decision Authority (MDA) Acquisition Support, EMCS Lead Standardization activity, E3 Awareness and Training, Joint Service Ordnance E3 program. Researches emerging spectrum technologies and develops analysis and simulation capabilities to assess spectrum supportability, manage spectrum use and promote effective spectrum operations.

J6 Spectrum Management Information Technology Division. -- supports the warfighter by providing and maintaining Spectrum Planning Services, E3 Models and Simulations, and Information Systems.

J7 Business Operations Division. -- manages all the personnel, financial, security and business planning requirements for the Joint Spectrum Center.

J8 Applied Engineering Division. -- provides technical (E3) and spectrum engineering analysis and test support on a customer-funded basis. This includes support to DoD and other Federal Government organizations; to the private sector when it is in the interest of national defense per 10 U.S.C 2539b; and to foreign entities when authorized by the Foreign Military Sales Process through the Defense Security Cooperation Agency.

JSC Tasks and Products: These include the following, JSC Liaison and Coordination Support to Information Operations and Electronic Warfare -- provides direct support to Unified Combatant Commands, Joint Task Forces, and Joint Staff Information Operations/Electronic Warfare (IO/EW) cells, and indirect support for operational military IO/EW planning provided through the Joint Information Operations Center (JIOC), Service IO activities, and IO/EW elements of the Intelligence Community. This effort is conducted under the mission area of "supporting electronic protect missions of information warfare as they relate to spectrum supremacy". The support provided ranges from EW de-confliction analyses to supporting IO red team efforts as they relate to spectrum dependent matters.

Support to the Warfighting Unified Combatant Commands and JTF Commanders -- includes:

- Support to the Electronic Warfare officer and the information operations (IO) cell JSC liaison and coordination support to IO cell, Joint Information Operations Center (JIOC), and Intelligence organizations as required
- Automated frequency management support and training, electromagnetic environmental database support, electromagnetic compatibility (EMC) analysis support
- Generation of the Joint Communications Electronics Operation Instruction (JCEOI)
- Development of the Joint Restricted Frequency List (JRFL)
- Joint Spectrum Interference Resolution (JSIR) support through analysis and deployment teams as necessary
- Area Studies in support of Unified Combatant Command requirements (see below)
- Review of operations plans (OPLANS) for spectrum supportability, upon request.

Area Studies in Support of Unified Combatant Command Requirements. Each year, the Joint Spectrum Center (JSC) produces area studies for various countries, on CD-ROM, that provide information on the physical and cultural characteristics and the civil telecommunications sector. Specific items addressed include: frequency management; broadcasting; telephone, telegraph, and telex; data communications; aeronautical communications; maritime communications; and transmission systems. Frequency allocations, assignments, histograms, and site location maps are also included. Frequency assignment data is also provided on the CDROM in a spreadsheet.

Electromagnetic Battlespace and Communications-Electronics Planning Support: supports achieving information superiority and full spectrum dominance by providing services and products to Assistant Secretary of Defense for Networks and Information Integration (NII), Joint Staff, Unified Commands, Joint Task Forces, Military departments, and Defense Agencies to enable the DoD's effective use of the electromagnetic spectrum.

Providing electronic battlespace and C-E planning support directly to the warfighter, the JSC Operations Division offers these typical services:

- SPECTRUM XXI Frequency Nomination/Assignment/Allotment
- Electronic Warfare De-confliction
- Joint Restricted Frequency List (JRFL) Assistance/Preparation
- Interference Analysis
- Propagation Predictions (MF-EHF)
- C-E System Performance Prediction
- Radar Target Acquisition Coverage Prediction
- EMC Analyses in Support of Frequency Planning
- Topographical Analyses
- JCEOI Planning/Preparation
- Electromagnetic Environment (EME) Definition
- Geophysical Environment Definition.

Joint Spectrum Interference Resolution (JSIR): Established by DoD in October 1992 as a replacement for the electromagnetic interference portion of the former DoD Meaconing*, Intrusion, Jamming, and Interference (MIJI) program. MIJI's focus was on the reporting of potentially hostile electronic warfare attacks against U.S. military systems. The JSIR program is structured to have interference incidents resolved at the lowest possible level of the component chain of command, using component organic resources to resolve interference incidents where possible. Those incidents that cannot be resolved locally are referred up the chain of command, with resolution attempted at each level. If the interference incident cannot be resolved by the affected DoD Component or the service engineering agency responsible for spectrum interference resolution, then it is referred to the JSC JSIR office for resolution.

C2-Protect Support: The JSC Operations Division supports C2-Protect operations through each of the following activities:

- Provision of databases on friendly force C2 system location and technical characteristics data for use in planning C2-protect. The databases cover DoD, US government, and civilian communications, as well as radar NAVAIDS, broadcast, identifications, and electronic warfare (EW) systems. The databases are available on a quick reaction basis in a variety of formats and media to meet the needs of IO planners and spectrum managers.
- Assistance to the EW officer or IO cell in the development of the JRFL. The JSC provides an automated tool, SPECTRUM XXI, to assist in the development and management of the JRFL. The JSC has Unified Combatant Command support teams that deploy to the combatant command or JTF. The teams are available to prepare the JRFL or provide training and assistance in JRFL preparation. These teams are also available to provide assistance in spectrum management matters.
- Assistance in the resolution of operational interference and jamming incidents through the auspices of the JSIR Program
- Provision of databases on foreign C3 frequency and location data. This data is developed primarily from open sources

- Provision of unclassified C3 area studies. The studies are unclassified, developed entirely from open source material, and address the C3 infrastructure of over 100 countries. The studies provide information on the physical and cultural characteristics (geography, climate, and population), overview of telecommunications systems, and the frequencies used by each country. Data is provided on civilian, military, radio/TV broadcast and navigational systems. The frequency data is provided in automated form and can be used directly by spectrum management tools such as the widely used SPECTRUM XXI.

Spectrum Regulatory Support. The growth of commercial wireless services, such as Personal Communications Services, has greatly increased the demand for spectrum, and increased pressure for the government to relinquish portions of the spectrum to commercial interests. Continuing pressure to reallocate portions of the spectrum requires that the DoD have the ability to quickly assess the operational and economic impact of proposed reallocation legislation in order to defend critical DoD spectrum. JSC draws upon a collection of databases and experience with spectrum management to respond to ad hoc inquiries. In addition, the JSC is positioned to develop in-depth assessments of various reallocation proposals that will provide all levels of government with the information needed to make responsible reallocation decisions.

Leadership: The command billet of the center (O-6) rotates between the Army, Air Force and Navy. The Commander, JSC reports to the Director, Defense Spectrum Organization who in turn reports to the DISA Vice Director.

Location: David Taylor Research Center, 2004 Turbot Landing, Annapolis, Maryland.

Phone: (410) 293-2456, DSN 281-2456

Website: <http://www.jsc.mil/>

Last updated: Oct 2007

Joint Warfare Analysis Center (JWAC)



Mission: provides combatant commands, Joint Staff, and other customers with precise technical solutions in order to carry out the national security and military strategies of the United States. JWAC maintains and enhances its ability to conduct comprehensive technical analysis. Over the past quarter of a century, JWAC has evolved from a small program office into a joint command of more than 600 personnel. As it grew, it became part of the Joint Chiefs of Staff in 1994 and then was spun-off as an independent joint command subordinate to Joint Forces Command (formerly Atlantic Command) in 1998.

Tasks:

- Provides Combatant Commander planners with full-spectrum analytical products in support of their objectives and guidance.
- Interfaces with the Joint Staff, national intelligence agencies, military commands, and governmental agencies to acquire necessary intelligence.
- Develops and adapts modeling and simulation technologies for analysis, computation, and the presentation of options to combatant commands, the Joint Staff, and other customers through partnership with Industry technology centers of excellence throughout DoD.
- Assesses strategic and operational planning processes including non-traditional methods for achieving national security objectives.

Capabilities:

- Maintains direct liaison staffs with Combatant Commanders, Joint Staff, DoD and non-DoD agencies. Liaison deploys in theater during crises and exercises.
- Researches political and socioeconomic conditions in countries of interest.
- Develops data-gathering and analysis methods and techniques to assess military, political, and socioeconomic impacts of U.S. military action and mathematical model and system simulations to support this analysis.
- Participates in development of new methodologies and technologies in support of joint experimentation, wargaming, and precision engagement.

Subordination: JWAC reports to the U.S. Joint Forces Command, Norfolk VA.

Leadership: Command of JWAC rotates between a Navy and Air Force O-6.

Personnel: The JWAC workforce is comprised of over 600 employees; approximately 500 are civilian and contractor positions, including multidisciplinary scientists, engineers, and analysts and the Command is authorized 62 military billets.

Location: JWAC is located at the Naval Support Facility, Dahlgren VA.

Note: The unclassified information above was obtained and approved by the JWAC for inclusion in this publication. Additional information may be obtained at:

Website: <http://www.jwac.mil/>

Last Updated: September 2007.

U. S. Strategic Command (USSTRATCOM)



U.S. Strategic Command (USSTRATCOM) is one of nine unified commands in the Department of Defense. It is located at Offutt Air Force Base near Omaha, Neb.. General Kevin P. Chilton commands USSTRATCOM, and serves as the senior commander of unified military forces from all four branches of the military assigned to the command. USSTRATCOM integrates and coordinates the necessary command and control capability to provide support with the most accurate and timely information for the President, the Secretary of Defense, other National Leadership and regional combatant commanders, and serves as steward and advocate of the nation's strategic capabilities.

USSTRATCOM is a global integrator charged with the missions of full-spectrum global strike, space operations, computer network operations, Department of Defense information operations, strategic warning, integrated missile defense, global C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance), combating weapons of mass destruction, and specialized expertise to the joint warfighter.

A command headquarters of more than 960 people, representing all four services, including Department of Defense civilians and contractors, oversees the command's operationally focused global strategic mission. The command is organized under a modified J-code structure as follows:

- **J0 The office of the Commander and the staff support agencies** - responsible for establishing the goals, mission, vision and leadership of the command. To help the commander, the immediate staff also includes the deputy commander in chief and a group of special advisors.
- **J1 (Manpower and Personnel)** - develops and administers USSTRATCOM command manpower and personnel policies, human resources, and personnel assignment programs.
- **J3 (Global Operations)** - coordinates the planning, employment and operation of DoD strategic assets and combines all current operations, global command and control and intelligence operations.
- **J2 (Intelligence)** - appraises the commander of foreign situations and intelligence issues relevant to current operational interests and potential national security policies, objectives and strategy. This includes providing indications, warning and crisis intelligence support, supporting unified command intelligence requirements, developing doctrine, developing joint architecture, coordinating support requirements and providing targeting support.
- **J3B (Current Operations)** - operates the Global Operations Center to provide the commander and the J3 with situational awareness, command and control, and integration across all mission areas. Conducts mission analysis, leads course of action development, and performs contingency and crisis action planning. Executes missions as directed by the Secretary of Defense and the President.
- **J4 (Logistics)** - Plans, coordinates and executes logistics functions for mobility, maintenance, engineering, readiness and sustainment and munitions management in support of command missions.

- **J6 (C4 Systems)** - coordinates, facilitates, monitors and assesses systems, networks and communications requirements.

- **J7 (Joint Exercises and Training)** - Manages USSTRATCOM Commander's Joint Training Program and Exercise Program in order to ensure readiness to perform the Command's Missions

- **J5 (Plans and Policy)** - responsible for coordinating the development and implementation of national security policy as it applies to the command and the execution of its mission. Develops future concepts and policy formulation for military space operations; global strike; information operations; global missile defense; and command and control, communications, computers, intelligence, surveillance and reconnaissance as outlined in the most recent Unified Command Plan. Integrates and synchronizes deliberate planning efforts across all USSTRATCOM missions. Prepares and maintains the nation's strategic nuclear war plan, and provides integrated global strike planning to deliver rapid, extended range, precision kinetic (nuclear and conventional) and non-kinetic (elements of space and information operations) effects in support of theater and national objectives. Performs day-to-day activities required for crisis-action and deliberate planning and execution, with updates to plans as necessary.

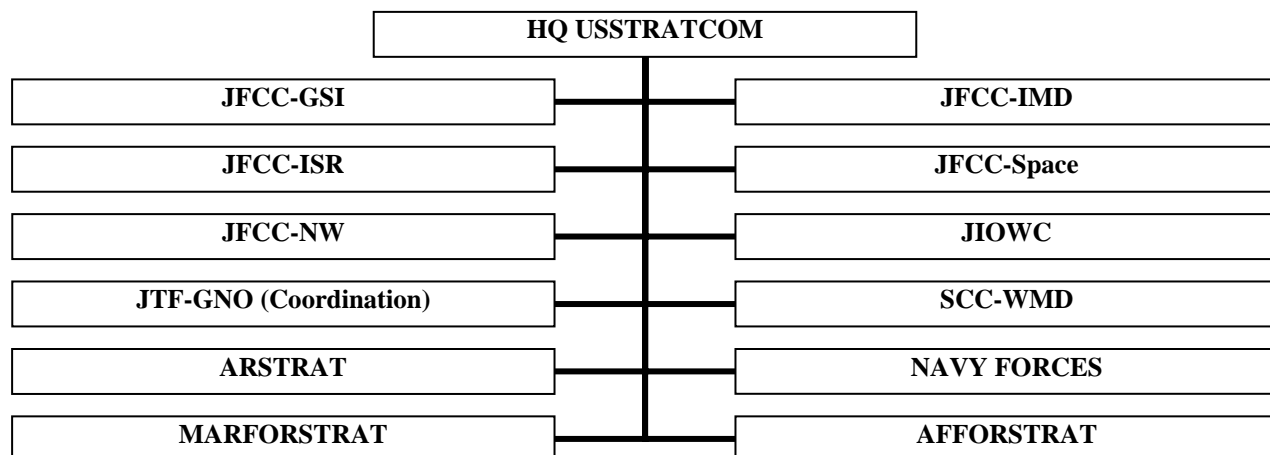
- **J8 (Capability and Resource Integration)** - conducts force management and analysis to include integrating, coordinating, prioritizing, and advocating USSTRATCOM future concepts, mission capability needs, weapons system development, support for emerging technologies, and command and control architecture across the mission areas. Responsible for the articulation and development of all command requirement processes to ensure that USSTRATCOM has the tools to accomplish its mission, and ensures appropriate decision support tools and assessment processes are in place to enhance operational capabilities. The directorate includes comptroller support, concepts and experimentation, and force assessments.

Global Innovation and Strategy Center (GISC) - The GISC mission is to produce knowledge discovery and shared understanding of strategic, operational and tactical perspectives to provide solutions to USSTRATCOM's toughest problems. The GISC is an academic facility that will bring together, in a cooperative effort, members of the public and private sector (military, political, academia, private sector, and media experts) and formalizes a process established soon after Sept. 11, 2001, with a focus on analyzing national and international security issues by leveraging expertise from the aforementioned elements of national power. This stimulates the development of innovative courses of action and comprehensive strategies to respond global threats against the United States.

USSTRATCOM exercises command authority over various task forces and service components in support of the command's mission. During day-to-day operations, service component commanders retain primary responsibility for maintaining the readiness of USSTRATCOM forces and performing their assigned functions. Their primary function is to provide organized, trained, and equipped forces for employment when called upon to support USSTRATCOM's global mission.

As the Department of Defense's key advocate for global capabilities, the command has extensive ties with defense agencies, the Department of Energy's national laboratories, and other sources of support. Through its many contacts and interagency relationships, the command facilitates planning, enhances information sharing between the military and other government agencies and streamlines decision making.

USSTRATCOM Functional Components, Service Components and Task Forces:



USSTRATCOM exercises command authority over five joint functional component commands (JFCCs) responsible for day-to-day planning and execution of primary mission areas: space and global strike; intelligence, surveillance and reconnaissance; network warfare; information operations; integrated missile defense; and combating weapons of mass destruction.

JFCC-Global Strike and Integration (GSI) -- optimizes planning, integration, execution and force management of assigned missions of deterring attacks against the U.S., its territories, possessions and bases, and should deterrence fail, by employing appropriate forces.

JFCC-Integrated Missile Defense (IMD) -- develops desired characteristics and capabilities for global missile defense operations and support for missile defense. Plans, integrates and coordinates global missile defense operations and support (sea, land, air and space-based) for missile defense.

JFCC-Intelligence, Surveillance and Reconnaissance (ISR) -- plans, integrates and coordinates intelligence, surveillance and reconnaissance in support of strategic and global operations and strategic deterrence. Tasks and coordinates ISR capabilities in support of global strike, missile defense and associated planning.

JFCC-Space (SPACE) -- optimizes planning, execution, and force management, as directed by the commander of USSTRATCOM, of the assigned missions of coordinating, planning, and conducting space operations.

JFCC-Network Warfare (NW) -- facilitates cooperative engagement with other national entities in computer network defense and network warfare as part of global information operations.

Joint Information Operations Warfare Command (JIOWC) -- plans, integrates, and synchronizes Information Operations (IO) in direct support of Joint Force Commanders and serves as the USSTRATCOM lead for enhancing IO across DoD.

Joint Task Force-Global Network Operations (JTF-GNO) -- directs the operation and defense of the Global Information Grid to assure timely and secure net-centric capabilities across strategic, operational, and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business missions.

USSTRATCOM Center for Combating Weapons of Mass Destruction (SCC-WMD) -- plans, advocates and advises the commander, USSTRATCOM on WMD-related matters. Provides recommendations to dissuade deter and prevent the acquisition, development or use of WMD.

For More information please visit www.stratcom.mil

Last Updated: October 2007

Joint Task Force – Global Network Operations (JTF - GNO)



MISSION: A component of U.S. Strategic Command (USSTRATCOM), the Joint Task Force – Global Network Operations (JTF-GNO), is located in Arlington, VA. Under the authority of USSTRATCOM, JTF-GNO has the mission of directing the operation and defense of the DoD's Global Information Grid (GIG) to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business missions.

HISTORY: By the mid to late 1990's, it became increasingly apparent that the Global Information Grid, also known as the GIG, and the DoD computer networks that control and operate within it were becoming increasingly vulnerable to attacks. The so-called "information superhighway" was rapidly becoming a "cyber battlefield" where the protection previously afforded by traditional geographical boundaries was diminished, and a threat to a single DoD computer system was now potentially a threat to all DoD computer systems.

The DoD recognized this growing cyber threat and in response created the Joint Task Force for Computer Network Defense (JTF-CND). JTF-CND achieved initial operational capability (IOC) on 30 December 1998 and full operational capability (FOC) in June 1999.

In October 1999, United States Space Command (USSPACECOM) assumed the CND Mission and JTF-CND was subordinated to it. In the fall of 2000, with the new Unified Command Plan (UCP) and the addition of an emerging Computer Network Attack (CNA) mission, JTF-CND began transforming into the Joint Task Force for Computer Network Operations (JTF-CNO).

JTF-CNO achieved IOC on 2 April 2001 and progressed towards achieving FOC on 1 October 2003. In October 2002, JTF-CNO was re-aligned under the United States Strategic Command (USSTRATCOM) under the new UCP, Change 2. JTF-CNO established itself as the premier DoD organization for intelligence analysis, planning, and operations of computer network warfare.

During its short history, JTF-CNO evolved from a handful of people to over 130 active duty military, civil service, and contracted employees. The JTF-CNO was instrumental in operationalizing computer network operations and defense for all of DoD. It also championed the CNA mission, working tirelessly to make this immature warfare area a viable part of our nation's ability to wage war.

In August 2003, JTF-CNO transformed its mission again with the transfer of the CNA mission to USSTRATCOM's Network Attack Support Staff (NASS). In January 2005, the mission to plan, integrate, coordinate and conduct CNA/CND, and integrate with CNE was given to Joint Functional Component Command – Network Warfare.

In June 2004, the JTF-CNO began its largest and most comprehensive transformation. On 18 June, the Secretary of Defense signed a delegation of authority letter designating the Director, Defense Information

Systems Agency (DISA) as the new Commander of Joint Task Force-Global Network Operations (JTF-GNO). With this designation, the new command assumed responsibility for directing the operation and defense of the GIG.

In July 2005, the JTF-GNO formed the Global NetOps Center (GNC) through the functional merger of elements from the JTF-CNO's Operations Directorate, DISA's Global Network Operations and Security Center (GNOSC), the DoD Computer Emergency Response Team (DoD-CERT), and the Global SATCOM Support Center (GSSC).

In May 2006 the UCP formally assigned CDRUSSTRATCOM the mission of directing GIG operations and defense-a mission subsequently assigned to the CDR JTF-GNO.

CURRENT OPERATIONS: The JTF-GNO performs its mission of directing the operations and defense of the GIG by using the NetOps construct that is outlined in its Joint Concept for GIG NetOps, Version 3, 4 Aug 06. NetOps is defined as the operational framework by which the CDRUSSTRATCOM, using his JTF-GNO component, will accomplish his assigned UCP (2006) mission of directing the operations and defense of the GIG. That framework consists of essential tasks, Situational Awareness, and Command and Control (C2). The essential tasks are GIG Enterprise Management (GEM), GIG Network Defense (GND), and GIG Content Management (GCM). Adhering to the responsibilities of the essential tasks (GEM, GND, and GCM) produces NetOps' desired effects of: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery in support of the overall goal of NetOps which is to provide the right information to the edge. NetOps and its essential tasks (GEM, GND, and GCM) include Information Assurance (IA) as defined and outlined in DODD 8500.1, Information Assurance, and CJCSI 6510.01E, Information Assurance and Computer Network Defense.

To execute these fundamental NetOps responsibilities, the CDR, JTF-GNO coordinates with Combatant Commands/Services/Agencies (CC/S/As). JTF-GNO has Operational Control (OPCON) over Service NetOps Components as provided in Forces For Memo, Feb 06, page IV-33, footnote 9 and stated in the Joint Concept of Operations for GIG NetOps, Version 3, 4 Aug 06. CDR, JTF-GNO also exercises Tactical Control (TACON) over the Service Computer Emergency / Incident Response Teams (CERTs/CIRTs) as provided in the Forces For Memo, Feb 06, page IV-33, footnote 9 and stated in the Joint Concept of Operation for GIG NetOps, Version 3, 4 Aug 06. To effectively operate the GIG as a global enterprise while realizing the Geographic Combatant Command (GCC) requirements to direct GIG operations in their theaters, CDRUSSTRATCOM developed an event-based C2 structure. C2 of GIG operations is based on the situation at the time. The three possible circumstances that determine the C2 of NetOps are known as global, theater, and non-global NetOps events. The preponderance of NetOps events are theater and are under the control of the GCC and their Service Components. Global and nonglobal NetOps events occur less frequently, but when they do occur, USSTRATCOM, using its JTF-GNO component, will direct the global response and respective CC/S/As will direct their non-global responses.

The Global NetOps Center (GNC) is the JTF-GNO Command Center responsible for executing the dailyoperation and defense of the GIG. The GNC provides the overall management, control, and technical direction for GIG NetOps and oversees a collaborative coordination process involving all Combatant Commands, Services, and Agencies, supporting the needs of the President, SECDEF, NetOps Community, and the warfighting, business, and intelligence domains.

Within each theater of operation, the JTF-GNO operates through Theater NetOps Centers (TNCs). The TNC is OPCON to JTF-GNO and offers onsite, theater support. Each TNC can issue technical directives to Service Theater Network Operations and Security Centers (STNOSCs)/Agency Theater Network Operations and Security Centers (ATNOSCs). The TNC develops, monitors and maintains a GIG SA view for the theater. The theater GIG SA view is aggregated and segmented based on requirements provided by the Theater NetOps Control Center (TNCC) as derived from the GIG common SA standards. The GIG SA view will include pertinent theater, operational, and tactical-level system and network,

GND, and GCM status.

The Service NetOps Component Commanders are the Commander, SMDC/ARSTRAT; the US Air Force Commander for USAF NetOps (USAF NetOps/CC); Commander, US Navy Network Warfare Command (USN NAVNETWARCOM); and Commander, US Marine Corps Network Operations and Security Command (MCNOSC). These Service Component Commanders exercises C2 over their respective Service Global Network Operations and Security Centers (SGNOSC).

The SGNOSCs and CERTs/ CIRTs serve as a part of the Service Component support to JTF-GNO. The SGNOSC and CERT/CIRT mission is to provide the Service-specific NetOps reporting and SA for the Service's portions of the GIG. The SGNOSC and CERT/CIRT provide worldwide operational and technical support to the Service's portions of the GIG across the strategic, operational, and tactical levels leveraging collaboration of the STNOSCs if established. The SGNOSC, in concert with the CERT/CIRT, are responsible for executing GND within their portion of the GIG, ensuring the Service's portions of GIG are secure and executing Service Title 10 enterprise responsibilities.

The Defense Agencies provide, operate, and maintain a large portion of the equipment, personnel, and other resources that make up the GIG. Execution of these functions requires the Agencies to be actively engaged in NetOps. To execute these functions, most Agencies have established NOSCs, which maintain SA of their portions of the GIG. The DoD Agencies that are not part of the Intelligence Community operate enterprise-wide systems as part of the GIG. These systems provide critical support to the DoD, COCOMs, and Military Services via their Agency Global NOSCs (AGNOSC). These AGNOSCs serve as a central point of contact for matters concerning the resources they provide to the GIG. DoD Agencies will align their AGNOSCs to provide USSTRATCOM visibility and insight of their GIG status and will follow the orders and directives issued by JTF-GNO per the 18 June 04 SECDEF Memo (modified by 17 Nov 05 DEPSECDEF Memo).

PERSONNEL: The JTF-GNO is currently authorized more than 300 positions.

Website: <https://www.jtfgno.mil> (PKI enabled website)

Website: www.stratcom.mil/fact_sheets/ (information only)

Last Updated: September 2007

This Page Intentionally Blank

Joint Information Operations Warfare Command (JIOWC)



Mission: JIOWC enables Information Operations (IO) and Strategic Communication (SC) for Joint Force Commanders. JIOWC coordinates and synchronizes regional and global IO/SC efforts and enhances IO/SC support across the Department of Defense.

Tasks:

- Provide continuous and integrated IO planning and execution support to JFCs, including COCOMs, JTFs, JFCCs, the JS, and the OSD. JIOWC will provide IO support to national agencies and organizations, allied nations or international organizations as directed.
- Conduct operational analysis which provides the foundation for IO planning within and across geographic regions.
- Assist in the integration of IO into joint exercises.
- Provide IO expertise to assist USSTRATCOM in IO force and capability development.
- Provide EW, PSYOP, MILDEC, and OPSEC expertise to COCOMs through Combatant Command Support Teams (CCSTs). JIOWC will train and field IO support teams capable of supporting the COCOMs IO staff with integrated IO planning during peacetime operations, contingencies, and exercises. JIOWC members will be deployment capable within 72 hours of formal notification.
- Provide OPSEC program development and training, assessment support, and plans and exercise support via the Joint OPSEC Support Center (JOSC) in coordination with the CCSTs.
- Provide MILDEC and long-range operational Mission Analysis via the Joint Mission Support Center (JMSC) in coordination with the CCSTs.
- Provide EW planning and execution support to JFCs via the Joint Electronic Warfare Center (JEWEC) in coordination with the CCSTs.
- Provide operational level strategic communication planning support to COCOMs, JFCs, and USSTRATCOM components via the Joint Strategic Communication Support Cell (JSSC) in coordination with the CCSTs.
- Serve as the USSTRATCOM lead for RC IO Integration across DoD.
- Serve as USSTRATCOM J8's lead agent for assisting the COCOMs in identifying and addressing their near term IO capability gaps.

- Act as the USSTRATCOM representative to and Co-Chair of the Joint IO Education Board of Advisors.
- Collaborate on course and curriculum development, and other key aspects of IO education and training with the Naval Postgraduate School and the Joint Forces Staff College (JFSC).

Capabilities:

- Deployable Combatant Commander support teams – tailored to augment J3 IO Cells
- Reachback – to satisfy Combatant Commander IO requirements with a small forward footprint
- Surge capability – to meet the demands of real world contingencies and exercises
- Visibility across commands – to share lessons learned, and to help synchronize teams regional effects
- IO simulation and planning tools - IOPCJ, JDSF, ION, RFMP, ARC-GIS and VISION

Subordination: The Joint Electronic Warfare Center (JEWEC) was established by the Secretary of Defense in October 1980 and reported to the Joint Staff. In September 1994, the mission was expanded and the organization was renamed the Joint Command and Control Warfare Center (JC2WC). In 1998, as a result of the Defense Reform Initiative (DRI), the JC2WC was realigned from the Joint Staff to US Atlantic Command. The JC2WC mission was further expanded and resulted in re-designation as the Joint Information Operations Center (JIOC). In October 1999, the JIOC was realigned as a subordinate command of USSPACECOM. On 1 October 2002, the JIOC was realigned as a subordinate command to USSTRATCOM. In July 2006 Commander USSTRATCOM approved the transformation of the Joint Information Operations Center to the Joint Information Operations Warfare Command (JIOWC). Commander JIOWC, reports to the Combatant Commander, USSTRATCOM.

Leadership: The Commander of the JIOWC is a nominative position that is filled by an USAF General, who is dual-hatted as the Commander, Air Force Intelligence, Surveillance and Reconnaissance Agency and Commander, Joint Information Operations Warfare Command.

Personnel: The JIOWC is currently authorized 210 positions. Three Allied officers and 160 contractors are fully integrated into the command.

Location: The JIOWC is co-located with the Air Force Intelligence, Surveillance and Reconnaissance Agency and the Air Force Information Operations Center (AFIOC) at Lackland AFB, TX.

Website: <http://www.jiowc.smil.mil>

Last updated: September 2007

U. S. Special Operations Command (USSOCOM)



USSOCOM is one of the nine U.S. unified commands under DOD. It organizes, trains, and equips special operations forces provided to Geographic Combatant Commanders, American Ambassadors and their country teams. USSOCOM manages and oversees all CONUS-based SOF from all four services. It also develops SOF-specific tactics, techniques, procedures, and doctrine, and conducts research, development, and acquisition of SOF-peculiar equipment. USSOCOM ensures its forces are trained and "joint-ready" to respond to the call from the President, Secretary of Defense and the other eight combatant commanders as necessary.

Mission. USSOCOM provides fully capable Special Operations Forces to defend the United States and its interests. USSOCOM plans and synchronizes operations against terrorist networks.

Special operations are operations conducted in hostile, denied, or politically sensitive environments to achieve military, diplomatic, informational, and/or economic objectives employing military capabilities for which there is no broad conventional force requirement. These operations often require clandestine or discreet capabilities. Special operations are applicable across the range of military operations. They can be conducted independently or in conjunction with operations of conventional forces or other government agencies and may include operations by, with, or through indigenous or surrogate forces.

Special Operations Forces Core Tasks

Counter-proliferation of weapons of mass destruction (WMD) – actions taken to locate, identify, seize, destroy or capture, recover, and render such weapons safe.

Counterterrorism – measures taken to prevent, deter, and respond to terrorism.

Foreign Internal Defense – providing training and other assistance to foreign governments and their militaries to enable the foreign government to provide for its country's national security.

Special Reconnaissance – acquiring information concerning the capabilities, intentions and activities of an enemy.

Direct Action – short-duration strikes and other small scale offensive actions taken to seize, destroy, capture, recover or inflict damage in denied areas.

Psychological Operations – operations that provide truthful information to foreign audiences that influence behavior in support of U.S. military operations.

Civil Affairs Operations – activities that establish, maintain or influence relations between U.S. forces and foreign civil authorities and civilian populations to facilitate U.S. military operations.

Unconventional Warfare – operations conducted by, through, and with surrogate forces that are organized, trained, equipped, supported, and directed by external forces.

Information Operations – operations designed to achieve information superiority by adversely affecting enemy information and systems while protecting U.S. information and systems.

IO Core and Related Capabilities within USSOCOM Purview:

Psychological Operations (PSYOP). A vital part of the broad range of U.S. political, military, economic, and information activities used by the U.S. government to secure national objectives, PSYOP disseminate truthful information to foreign audiences in support of U.S. policy and national objectives. Used during peacetime, contingency operations, and declared war, these activities are not a form of force, but are force multipliers that use nonviolent means in often violent environments. Persuading rather than compelling physically, they rely on logic, fear, desire or other mental factors to promote specific emotions, attitudes or behaviors. The ultimate objective of U.S. military psychological operations is to convince target audiences to take action favorable to the United States and its allies. The importance and effectiveness of psychological operations has been underscored during OPERATIONS ENDURING FREEDOM and IRAQI FREEDOM.

Civil Affairs (CA). CA units support military commanders by working to minimize the effect of civilians in the battle space and by coordinating with civil authorities and civilian populations in the commander's area of operations to lessen the impact of military operations on them during peace, contingency operations, and declared war. Civil Affairs forces support activities of both conventional and SOF, and are capable of assisting and supporting the civil administration in their area of operations. Long after the guns have fallen silent, the men and women of Civil Affairs continue to provide assistance to foreign governments, and to stabilize regions in turmoil.

Components. USSOCOM has four component commands and one sub-unified command:

1. U.S. Army Special Operations Command (USASOC). Located at Ft. Bragg, North Carolina. USASOC's mission is to organize, train, man, equip, educate, maintain combat readiness, and deploy assigned active duty and Reserve Components of the Army Special Operations Force. Their mission is to accomplish special operations, psychological operations, and civil affairs operations. Their forces include:

- - 4th PSYOP Group (4th POG)
 - 95th Civil Affairs Battalion
- United States Special Forces Command (Airborne).
- John F. Kennedy Special Warfare Center and School.

NOTE: Effective 1 Oct 06 the following units were reassigned from U.S. Special Operations Command (USSOCOM) to U.S. Joint Forces Command (USJFCOM):

- 350th, 351st, 352, and 353 Civil Affairs Commands (U.S. Army Reserve)
- 2nd POG and 7th POG (U.S. Army Reserve)

2. Naval Special Warfare Command (NAVSPECWARCOM). Located at Naval Amphibious Base, Coronado, CA. The mission of NAVSPECWARCOM is to organize, train, man, equip, educate, maintain combat readiness, and deploy assigned forces in support of joint and fleet operations worldwide. SEAL Teams are maritime, multipurpose combat forces organized, trained and equipped to conduct a variety of special missions in all operational environments and threat conditions. SEAL special mission areas include unconventional warfare, direct action, counter-terrorism, special reconnaissance, foreign internal defense, information warfare, security assistance, counter-drug operations, personnel recovery, and hydrographic reconnaissance.

3. Air Force Special Operations Command (AFSOC). Located at Hurlburt Field, Florida. It provides Air Force Special Operations Forces for worldwide deployment and assigned to geographic unified commands, conducting the full spectrum of special operations core tasks. AFSOC's contribution to Information Operations is specifically in the form of the 193^d Special Operations Wing, Air National Guard. The wing operates the EC 130 "Commando Solo" which can broadcast television and radio programs directly to foreign audiences.

4. Marine Corps Forces Special Operations Command (MARSOC). Located at Camp Lejeune, NC. Activated February 2006, its primary mission is to organize, man, train and equip Marine Special Operations Forces. The MARSOC subordinate elements provide training to foreign militaries, conduct specified special operations missions like special reconnaissance, engage in direct action, provide intelligence support, coordinate supporting fires and provide logistical support to special operations task forces.

5. Joint Special Operations Command (JSOC). A sub-unified command of USSOCOM. JSOC provides a joint headquarters to study special operations requirements, ensures interoperability and equipment standardization, develops joint special operations plans and tactics, and conducts joint special operations exercises and training.

Location Address and Contact Information: Headquarters, United States Special Operations Command (HQ, USSOCOM)

- Headquarters, USSOCOM, 7701 Tampa Point Boulevard, MacDill Air Force Base, Florida 33621
- Public Affairs Office: (813) 828-4600

Website: <http://www.socom.mil/>

Last Updated: October 2007

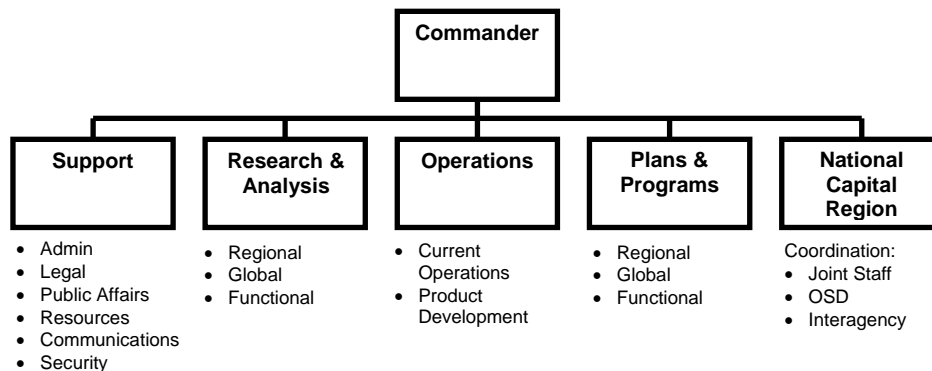
This Page Intentionally Blank

Joint PSYOP Support Element (JPSE)



History: The JPSE was established in 2003 and formally activated in 2006 at U.S. Special Operations Command (USSOCOM), Tampa, Florida. Shortly after September 11th, 2001, the Office of the Secretary of Defense (OSD) articulated a need for a strategic PSYOP capability within the Department of Defense (DoD). The Defense Planning Guidance (FY 2004-2009) tasked Commander, USSOCOM to create a “Strategic PSYOP Force.” The 2003 DOD Information Operations Roadmap directed the creation of “a Joint PSYOP Support element.” On 28 February, 2007, GEN Brown, Commander, USSOCOM, designated in writing that the JPSE was a subordinate Joint Command of USSOCOM with OPCON to Director, Center for Special Operations.

Mission: The Joint PSYOP Support Element (JPSE) plans, coordinates, integrates and, on order, executes trans-regional psychological operations to promote U.S. goals and objectives.



Commander's Intent:

- Deny safe-haven to terrorists abroad
- Counter or defeat global terrorist ideology and influence
- Plan, develop, coordinate, synchronize, and on order execute PSYOP at the global and trans-regional level
- Support the Global War on Terrorism (GWOT) mission of: USSOCOM, USSTRATCOM, Geographic Combatant Commanders (GCCs), Joint Staff, OSD, and the Interagency
- Provide sophisticated, commercial quality PSYOP support

Characteristics:

- One of two brigade-level PSYOP units assigned to USSOCOM
- Comprised largely of senior military and civilian PSYOP personnel
- Provides professional analysis and planning
- Provides commercial-quality PSYOP prototype development

- Develops DoD trans-regional PSYOP plans and can assist in developing COCOM/JTF Strategic Communication, Information Operations, and PSYOP plans
- Coordinates trans-regional dissemination, ensuring integration with deployed PSYOP units

Source: Director of Operations, 813-828-0430/6620

Last Updated: September 2007

Joint Public Affairs Support Element (JPASE)



Mission: The Joint Public Affairs Support Element (JPASE) trains and maintains a public affairs professional capability to rapidly deploy as a team to assist the combatant commanders. The operational teams help to properly disseminate information to the public. JPASE seeks to enhance overall joint public affairs capabilities through not only training but also doctrine development, and the establishment of joint standards and requirements to assure the joint force commander has an organization of equipped, trained and ready public affairs professionals. The goal is for these professionals to provide counsel, operational planning and tactical execution of communication strategies as a function of joint military operations in support of national objectives. JPASE is located in U.S. Joint Forces Command's (USJFCOM) Joint Warfighting Center (JWFC) in Suffolk, Va.

JPASE Mission Statement: The Joint Public Affairs Support Element assures Joint Force commanders Public Affairs forces through joint capability development and training to plan and execute communication strategies in the joint, interagency and multinational environments. When directed, JPASE deploys in support of Combatant Commanders worldwide.

JPASE is organized to provide direct support to specific combatant command requirements. It replaces the former, *ad hoc* method of assembling teams to provide support. This new organization facilitates concentration on the particular aspects of geography, culture and organization of a specific command, while gaining proficiency and understanding of the common operating tools and practices each command employs. On order, JPASE deploys to the regional Combatant Commands in support of emergent joint operations as a trained, equipped and ready joint public affairs force. Its first deployment was during Hurricane Katrina in 2005. Forty-six of JPASE's 48 military and civilian personnel, drawn from all services, are designated to support expeditionary operations.

Organization: JPASE is organized around three objective areas:

1. **Proponency Division:** The Proponency Division is responsible for developing and sustaining capability improvements across the areas of doctrine, organization, training, materiel, leadership & education, personnel, and facilities, and is divided into seven functional areas:

- Concept development and experimentation
- Visual information development
- Public affairs collaborative information environment/Web portal management
- Lessons learned
- Education development
- Doctrine and Policy
- Capabilities

2. Operations and Training Division: The operations and training division is responsible for training public affairs and operational staffs includes four teams, geographically aligned with the unified commands, providing public affairs training, media simulation, staff assistance and exercise support to those commands.

3. Expeditionary Capability: The JPASE provides a standing, rapidly-deployable, turn-key joint public affairs capability to support a variety of operational requirements. Each of the operational training teams form the core of a Scalable Public Affairs Response Capability (SPARC) – a ready, mission tailored force package, to support exercises and to deploy in support of the combatant commands for operations and contingencies. COCOMs must provide logistics and life-support to each SPARC. At full operational capability (FOC) JPASE can deploy up to 24 persons for 90 days or 16 for 179 days and still maintain its ability perform all its mission essential tasks.

Reserve Components Capability: USJFCOM established a reserve joint public affairs unit (JPASE-R), in October 2004 to support and augment the active duty JPASE organization. It is trained and equipped to provide training and support for the active JPASE force during day-to-day operations and when it is deployed in support of emergent and contingency operations. It will be certified to deploy in support of operations, in whole, in part, or as individual augmenters.

Website: JFCOM Joint Warfighting Training Center: http://www.jfcom.mil/about/abt_j7.htm

Last Updated: September 2007

Joint Forces Staff College Information Operations Program



The Joint Forces Staff College (JFSC) was established in 1946 to better equip personnel from all of the services to function in the modern joint and combined warfare environment. It pre-dates the creation of the unified Department of Defense, and is the successor of the Army and Navy Staff College, established in 1943 for the same purpose. The college is located at the U.S. Naval Base, Norfolk, Virginia.

IO Education at JFSC. Department of Defense Instruction (DODI) 3608.12, “ Joint Information Operations (IO) Education”, (4 Nov 05) specifies that, “Joint Forces Staff College [will] develop and conduct a Joint IO planners course to prepare students to integrate IO into plans and orders on joint warfighting staffs”. The College also offers an orientation course. Both are conducted by the Information Operations Division of the Joint Command, Control & Information Operations School (JC2IOS), and are outlined below.

1. Joint IO Orientation Course (JIOOC)

A one week course with the objective to educate and train U.S. Government (USG) personnel in the military grades of Lieutenant/Captain (O-3) to Captain/Colonel (O-6) and civilian equivalents in the basics of joint Information Operations (IO). Primary emphasis is at the Combatant Command level. The course focuses on teaching joint IO doctrine and DoD IO policy guidance as they apply to the operational level of joint warfare. It is particularly relevant to those serving in support of IO cells and other staff positions that require a basic knowledge of Joint IO. If IO planning skills are desired, then the student should take the JIOPC.

It gives students a common baseline of IO knowledge upon which to build practical skills and abilities to employ IO tools and techniques. In this one-week course, students are exposed to four blocks of instruction: Strategy; Intelligence support; IO Capabilities (Core, Supporting and Related); and Organization, Training, and Equipping. Each block of instruction includes a combination of instructor lecture, guest speaker presentations, guided discussions and/or panel discussions.

2. Joint Information Operations Planning Course (JIOPC)

A four week course for the purpose of establishing a common level of understanding for IO planners and IO capability specialists, between the ranks of O-4 through O-6, and DoD Civilian equivalents, who will serve in joint operational-level IO billets. *This course is a prerequisite for personnel assigned to the Joint IO career force* (See DODI 3608.11, Information Operations Career Force , 4 Nov 05).

The objective of the JIOPC is to educate and train military students between the ranks of O-4 through O-6, and DoD Civilian equivalents, to plan, integrate, and synchronize full spectrum IO into joint operational-

level plans and orders. The school accomplishes this through class presentations, guest lectures, case studies, and practical exercises in a joint seminar environment. Students will be assigned to a working group consisting of approximately eight to ten individuals led by a faculty mentor. The course focuses on the following six (6) learning areas:

- Joint Operations Planning and Execution System (JOPES)
- Joint Intelligence Preparation of the Environment
- IO Planning
- Interagency Planning & Coordination
- Military Deception (MILDEC)
- Operations Security (OPSEC)

Throughout the course the students use traditional planning methodologies within the joint planning community. The course is based upon joint doctrine that is reinforced, when necessary, by a compilation of various tactics, techniques, and procedures from throughout the department of defense.

The JIOPC is only taught in residence at the Joint Forces Staff College, but is also offered 1-2 times per year at the Joint Information Operations Center in San Antonio, TX. JIOC staff and Combatant Command IO planning teams have priority for available seats.

For information regarding the JFSC Information Operations Division, contact JC2IOS-IO@jfsc.ndu.edu or at 757-443-6339 (DSN: 646)

Web Site http://www.jfsc.ndu.edu/schools_programs/jc2ios/default.asp

Last Updated: September 2007

Information Operations Center of Excellence, Naval Postgraduate School



Mission. The President, Naval Postgraduate School (NPS) was tasked by Department of Defense Instruction (DoDI) 3608.12, (“Joint Information Operations (IO) Education” - 4 Nov 05) with establishing a DoD “Center of Excellence” (CoE) for Information Operations.

The IO CoE functions under the sponsorship of Commander, US Strategic Command (USSTRATCOM) to inform and support the development of innovations in Information Operations related policy, doctrine, technology and education.

History of NPS. NPS is located in Monterey, CA and is the successor to the Postgraduate Department of the U.S. Naval Academy, established at Annapolis, MD prior to World War One. Congress established the school as a full degree-granting institution in 1945, and it moved to its present location in 1951. The present student body numbers approximately 1,800, with representatives from all service branches, and the services of more than 25 allied nations. It grants degrees at the masters and doctorate levels.

Information Operations Education at NPS

1. ISO Fundamentals Certificate Program. NPS offers this certificate program on line, which is Phase 1 of its Master of Science (MS) degree in Information Systems and Operations (ISO). The certificate program consists of four-courses given via Distributed Learning (DL). These four courses are:

SS3011 - Space Technology and Applications

IO3100 - Information Operations

IS3502 - Computer Networks: Wide Area/Local Area (Intro to Information Systems Networks)

CC3000 - Intro to Command , Control, Communication, Computer and Intelligence Systems in DoD

IO3100 - Information Operations provides a survey of Information Operations (IO) along the time line of peace, to conflict, and back to cessation of hostilities. Students study the methods and elements which contribute to successful Information Operations including: Psychological operations and deception, Operational security, information assurance, and infrastructure protection, Electronic attack/protect/support, Physical attack/destruction in support of IO, Military-civilian relationship, Human cognition and decision making, Command and control structures, Legal issues, Computer and network attack, Systems engineering concepts (including modeling and simulation), Sensor and signals intelligence support to IO.

2. Master of Science in Information Systems and Operations (Curriculum 356). This is a war-fighter oriented, MS degree, in-residence program that will provide fundamental graduate education to integrate information technologies, command and control processes, and IO methods and elements into innovative operational concepts for Information Operations in the context of Network Centric Warfare.

The Information Systems & Operations graduate will be able to:

- Innovatively create IO strategies and policies.
- Establish agile organizational structures and decision processes responsive to real time mission and situation requirements.
- Understand information technology and systems as enabling the acquisition of information and knowledge superiority leading to effective development and performance of information operations.
- Integrate technology, organization, policy and strategy into an Information Operations framework useful in both deliberate and crisis planning across the range of military operations;
- Identify and solve significant information operations problems and communicate the results in written reports and command briefings.

Website: Information on Naval Postgraduate School's ISO program can be obtained at the following site:
http://www.nps.edu/DL/NPSO/cert_progs/iso.html

3. Master of Science in Information Warfare Systems Engineering (Curriculum 595). Graduates of this curriculum are thoroughly knowledgeable in Information Operations (IO) and Information Warfare (IW). They receive a Master of Science in Information Warfare Systems Engineering (MSIWSE) degree that provides the services with officers who are well versed in the technical, theoretical, and operational aspects of interdisciplinary IO/IW as they relate to joint mission objectives in modern warfare. This curriculum is co-sponsored by the Joint Staff (J39) and Commander, Naval Network Warfare Command, Information Operations Directorate.

Website: Information on Naval Postgraduate School's MSIWSE program can be obtained at the following site: <http://www.nps.edu/Academics/GeneralCatalog/414.htm#o436>

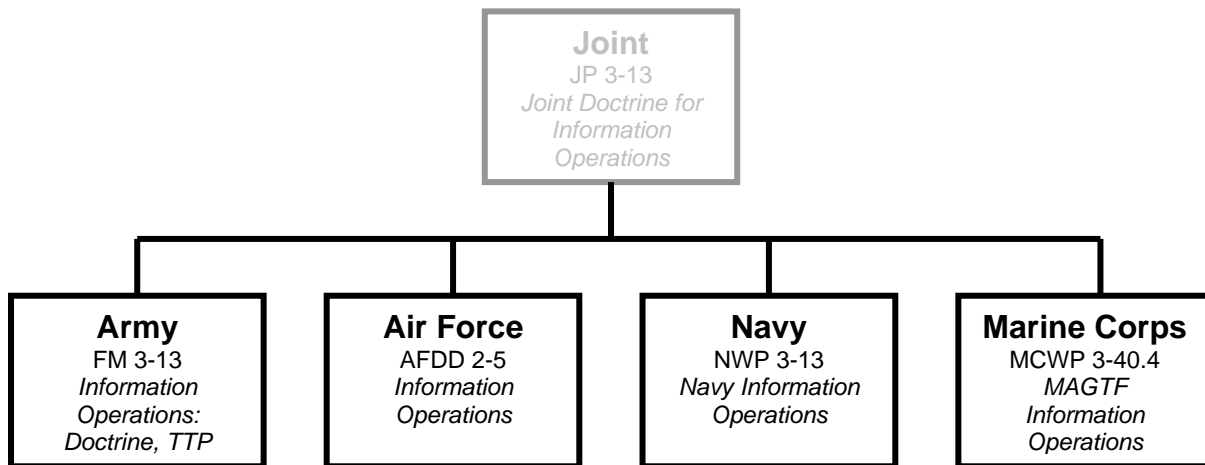
4. Master of Science in Joint Information Operations (Curriculum 698.) The Joint Information Operations curriculum educates military personnel and civilian officials in the strategic and operational dimensions of information relative to the use of force as an instrument of statecraft. Graduates will be able to develop information strategies to support military action by taking advantage of information technology, exploiting the growing worldwide dependence on automated information systems and capitalizing on near real time global dissemination of information to affect adversary decision cycles with the goal of achieving information superiority. This capability is possible only after students develop a thorough understanding of the enduring nature of war.

The curriculum is designed for both the specialist who will be assigned to an information operations position and the generalist who will be assigned to an operations directorate. The curriculum includes a core of military art and operations, the human dimension of warfare (psycho-social), analytical methods, and a technical sequence customized for each student. Additionally, each student will have an elective sequence designed to further develop an in-depth understanding of joint information operations. Graduates are awarded a Master of Science in Joint Information Operations. The program is 18 months long and requires a completed thesis.

Website: Information on the JIO Curriculum can be obtained at the following site:
<http://www.nps.navy.mil/da/>

Last Updated: September 2007

Service Information Operations Doctrine



This Page Intentionally Blank

Army Information Operations Doctrine



U.S. Army Information Operations doctrine is under review and a new edition of FM 3-13 is being drafted. This section reflects the currently published doctrine.

Key doctrinal documents: FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, 28 November 2003

Excerpts of Army Doctrine - FM 3-13

Introduction

Information operations (IO) encompass attacking adversary command and control (C2) systems (offensive IO) while protecting friendly C2 systems from adversary disruption (defensive IO). Effective IO combines the effects of offensive and defensive IO to produce information superiority at decisive points.

IO brings together several previously separate functions as IO elements and related activities. IO elements include the IO core capabilities, specified supporting capabilities, and related activities discussed in chapter 1. It also allows commanders to use all of them both offensively and defensively, as they deem appropriate. The assistant chief of staff (ACOS) G-7 has the coordinating staff responsibility for coordinating IO elements and related activities. This enables the G-7 to shape the information environment to friendly advantage and protect commanders and friendly C2 systems from adversary IO.

Offensive IO destroy, degrade, disrupt, deny, deceive, exploit, and influence adversary decision-makers and others who can affect the success of friendly operations. Offensive IO also target the information and information systems (INFOSYS) used in adversary decision-making processes.

Defensive IO protect and defend friendly information, C2 systems, and INFOSYS. Effective defensive IO assure friendly commanders an accurate common operational picture (COP) based not only on a military perspective, but also on nonmilitary factors that may affect the situation. An accurate COP is essential to achieving situational understanding. (See FM 6-0.) Most IO elements may be used either offensively or defensively. Effective IO requires integrating IO related activities—such as, public affairs and civil military operations—into IO as well.

Information Operations Doctrine

Commanders conduct (plan, prepare, execute, and assess) information operations (IO) to apply the information element of combat power. Combined with information management and intelligence,

surveillance, and reconnaissance operations, effective IO results in gaining and maintaining information superiority. Information superiority creates conditions that allow commanders to shape the operational environment and enhance the effects of all elements of combat power. IO has two categories, offensive IO and defensive IO. Commanders conduct IO by synchronizing IO elements and related activities, each of which may be used either offensively or defensively. Army IO doctrine supports joint IO doctrine, supplementing it where necessary to meet the conditions of land operations.

1. Design of Army Information Operations

Information operations (IO) bring together several previously separate functions as IO elements and related activities. To provide unity of effort, IO is placed under a special staff officer, the assistant chief of staff G-7. ... The G-7 has coordinating staff responsibility for IO. He does this by means of the G-7 section and IO cell. Placing responsibility for synchronizing the activities of the IO elements and related activities on one special staff officer helps commanders mass their effects to gain and maintain information superiority.

- **Information Environment**

The *information environment* is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself (JP 3-13). It includes — • The worldwide interconnection of communications networks. • Command and control (C2) systems of friendly and adversary forces and other organizations. • Friendly, adversary, and other personnel who make decisions and handle information. Climate, terrain, and weapons effects (such as electromagnetic pulse or blackout) affect the information environment but are not part of it.

Threat sources [include:] hackers, insiders, activist nonstate actors, terrorists, foreign IO activities, and information fratricide.

Methods of attack include: unauthorized access, malicious software, electromagnetic deception, electronic attack, physical destruction, and perception management.

- **Information Superiority**

The Army defines *information superiority* as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (FM 3-0). This definition differs slightly from the joint definition. While joint doctrine considers information superiority a capability, Army doctrine establishes it as an operational advantage. For Army forces, information superiority describes the degree of dominance that commanders have over the part of the information environment that affects their operations, and over the adversary. Commanders measure it in terms of information- based activities. Gaining and maintaining information superiority creates conditions that allow commanders to shape the information environment and enhance the effects of other elements of combat power. Commanders direct three interdependent contributors to achieve this goal:

- **Information management** is the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision-making. It uses procedures and information systems to collect, process, store, display, and disseminate information (FM 3-0). Information management (IM) consists of INFOSYS (see paragraph 1-6) and relevant information (RI).
- **Intelligence, Surveillance, and Reconnaissance (ISR)** an enabling operation; integrates and synchronizes all battlefield operating systems to collect RI to facilitate commander's decision-making.

- **Information Operations Contributions.** IM, IO, and ISR each have a different focus. ISR collects data and produces intelligence. IM disseminates and uses RI throughout the C2 system. IO applies that RI to protect the friendly C2 system, attack the adversary C2 system, and shape the information environment. All are essential to achieving and maintaining information superiority.

- **Aspects of Information Operations**

Information operations is the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making. (This definition supersedes the definition of IO in FM 3-0. It is consistent with joint initiatives.) [Editor's Note: It is also different from the current Joint definition.]

- **Elements of Information Operations**

IO are enabling operations that create and present opportunities for decisive operations. Commanders use both offensive IO and defensive IO simultaneously to accomplish the mission, increase their force effectiveness, and protect their organizations and systems. IO elements include core capabilities and supporting capabilities [see table below]. Commanders conduct IO through a combination of these elements and related activities.

The elements of IO are not organizations. They are independent activities that, when taken together and synchronized, constitute IO. Commanders decide which IO elements are appropriate to accomplish the mission. All elements may not be required for each operation.

With the possible exceptions of computer network operations (CNO), CNA, computer network defense (CND) and computer network exploitation (CNE), no IO element is new. What is new is bringing these elements/related activities together as components of the information element of combat power. IO focuses efforts that before were diffuse. A single staff officer—the G-7—is assigned authority and responsibility for these previously separate activities. This allows commanders to mass the effects of the information element of combat power.

IO related activities include but are not limited to public affairs (PA) and CMO. Although FM 3-13 discusses only these two, any activity that contributes to gaining and maintaining information superiority (for example, an operation in support of diplomatic efforts conducted by special operations forces) may be considered an IO related activity.

Core	Supporting
<ul style="list-style-type: none"> • Electronic warfare • Computer network operations <ul style="list-style-type: none"> ○ Computer network attack ○ Computer network defense ○ Computer network exploitation • Psychological operations • Operations security • Military deception 	<ul style="list-style-type: none"> • Physical destruction • Information assurance • Physical security • Counterintelligence • Counterdeception • Counterpropaganda <p>Editor's Note: Subordinate elements of CNO are indented in the table for clarity.</p>

Information Operations Elements

- **Army-Joint Information Operations Relationships**

IO, by their nature, are joint operations. Each Service component contributes to an integrated whole synchronized by the joint force headquarters. The IO cell at joint force headquarters deconflicts and synchronizes joint force IO. All Service components are represented. The joint force IO cell

synchronizes all the Service-specific IO elements/related activities to achieve unity of effort supporting the joint force. Army forces submit requests for IO support from joint force or higher echelons through the senior Army headquarters to the joint force IO cell.

○ **Offensive Information Operations**

The Army defines *offensive information operations* as the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision-makers or to influence others to achieve or promote specific objectives (FM 3-0). The Army definition deletes a sentence in the joint definition that lists IO elements associated with offensive IO. Army doctrine allows commanders to use all IO elements offensively.

Offensive IO facilitates seizing and retaining the initiative by creating a disparity between the quality of information available to friendly forces and that available to adversaries. The following effects create this information advantage:

- **Destroy.** *Destroy* is to damage a combat system so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt (FM 3-90). Destruction is most often the use of lethal and nonlethal means to physically render adversary information useless or INFOSYS ineffective unless reconstituted.
- **Disrupt.** *Disrupt* is a tactical mission task in which a commander integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt his timetable, or cause his forces to commit prematurely or attack in a piecemeal fashion (FM 3-90). *Disrupt*, in information operations, means breaking or interrupting the flow of information between selected C2 nodes.
- **Degrade.** *Degrade*, in information operations, is using nonlethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems, and information collection efforts or means. Offensive IO can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.
- **Deny.** *Deny*, in information operations, entails withholding information about Army force capabilities and intentions that adversaries need for effective and timely decision-making. Effective denial leaves opponents vulnerable to offensive capabilities. OPSEC is the primary nonlethal means of denial. It applies throughout the spectrum of conflict.
- **Deceive.** *Deceive* is to cause a person to believe what is not true. Military deception (MD) seeks to mislead adversary decision-makers by manipulating their understanding of reality. Successful deception causes them to believe what is not true.
- **Exploit.** *Exploit*, in information operations, is to gain access to adversary command and control systems to collect information or to plant false or misleading information.
- **Influence.** *Influence* is to cause adversaries or others to behave in a manner favorable to Army forces. It results from applying perception management to affect the target's emotions, motives, and reasoning. Perception management also seeks to influence the target's perceptions, plans, actions, and will to oppose friendly forces.

○ **Defensive Information Operations**

The Army defines *defensive information operations* as the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. 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 (FM 3-0). The Army definition deletes a sentence in the joint definition that lists IO elements associated with defensive IO. Army doctrine allows commanders to use all IO elements defensively.

Defensive IO seeks to limit the vulnerability of C2 systems to adversary action and to prevent enemy interference with friendly information and INFOSYS. Defensive IO effects include: **protection, detection, restoration, and response.**

- **Protection.** *Protection* is all actions taken to guard against espionage or capture of sensitive equipment and information. In IO, protection occurs at the digital perimeter to control access to or mitigate the effects of adversary access to friendly decision-makers and INFOSYS.
 - **Detection.** *Detection* is to discover or discern the existence, presence, or fact of an intrusion into information systems. Detection is the identification of adversary attempts to gain access to friendly information and INFOSYS.
 - **Restoration.** *Restoration* is to bring information systems back to their original state. Restoration is reestablishment of essential capabilities of INFOSYS damaged by enemy offensive IO.
 - **Response.** *Response* in information operations is to react quickly to an adversary's information operations attack or intrusion. Timely identification of adversaries, their intent and capabilities, is the cornerstone of effective response to adversary offensive IO.
- **Relationship of Offensive and Defensive Information Operations**
- Commanders synchronize offensive and defensive IO to produce complementary and reinforcing effects (see FM 3-0). Offensive IO supports the decisive operation, while defensive IO protects friendly force critical assets and centers of gravity. Conducting offensive and defensive IO independently detracts from the efficient employment of IO elements.
- **Information Operations Across the Spectrum of Conflict**

The national security and national military strategies establish an imperative for engagement (see FM 1). Engagement involves the nation exercising the instruments of national power—diplomatic, informational, military, and economic—to shape the security environment. ... Throughout the spectrum of conflict, commanders conduct IO to apply the information element of combat power. In all situations, Army forces do not act in isolation. Almost all operations are joint; most are interagency as well.

- **Peace.** During peace, commanders conduct IO to shape the strategic environment or to prepare for operations during crisis and war. Normally IO are part of a combatant commander's theater engagement plan. The majority of peacetime preparation is done at home station or during training exercises.
- **Crisis.** During crises, Army forces conduct IO based on existing contingency plans or a crisis action plan (see JP 5-0). A potential or actual contingency requires commanders at all echelons to gather additional information and refine their contingency plans based on a specific AO or target set. Geographic combatant commanders may use the relationships and conditions in the information environment created during peace to influence potential adversary decision-makers to act in ways that will resolve the crisis peacefully.

- **War.** During war, commanders conduct IO to synchronize the information element of combat power with the other elements of combat power. Well-synchronized offensive IO can cripple not only adversary military power but also adversary civilian decision-making capability. Commanders and staffs follow the military decision-making process to plan IO that accomplishes the commander's intent and concept of operations.
- **The G-7 Section and the Information Operations Cell**

The G-7 has coordinating staff responsibility for IO. He does this by means of the G-7 section and IO cell. The G-7 section has assigned officers and NCOs responsible for IO current operations, IO planning and IO targeting... The G-7 coordinates IO related activities of other staff officers through the IO cell.

The IO cell, located in the main command post, brings together representatives of organizations responsible for all IO elements and related activities. Related activities include any organizations able to contribute to achieving IO objectives. PA and CMO are always related activities; commanders may designate others. The IO cell also includes representatives of special and coordinating staff sections, as the mission requires. All battlefield operating systems are represented. The primary function of an IO cell is to synchronize IO throughout the operations process. In corps and divisions, the G-7 section forms its nucleus. In Army service component commands (ASCCs), the plans, current operations, and effects control divisions—under the deputy chief of staff for operations—coordinate IO. The ASCC ensures Army IO supports the theater IO campaign plan. If another headquarters is designated as the ARFOR, that headquarters assumes this responsibility

2. Information Operations Elements and Related Activities

The core and supporting IO elements are similar to the battlefield operating systems. They are independent activities that, when taken together and synchronized, constitute IO.

- **Core Elements**

Core IO elements are operations security (OPSEC), psychological operations (PSYOP), military deception (MD), electronic warfare (EW) and computer network operations (CNO). ***Computer network operations comprise computer network attack (CNA), computer network defense (CND), and related computer network exploitation (CNE) enabling operations.***

PSYOP, MD and OPSEC are employed to influence adversary decision-makers or groups while protecting friendly decision-making. EW and CNO are employed to affect or defend the electromagnetic spectrum, information systems (INFOSYS), and information that support decision-makers, weapon systems, command and control (C2), and automated responses.

- **Operations Security**

The Army defines *operations security* as a process of identifying essential elements of friendly information and subsequently analyzing friendly actions attendant to military operations and other activities to --

- Identify those actions that can be observed by adversary intelligence systems.
- Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive essential elements of friendly information time to be useful to adversaries.

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

- **Psychological Operations**

Psychological operations are planned operations that convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately to influence the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives (JP 3-53).

- **Military Deception**

Military deception comprises actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (JP 3-58). It is used to make an adversary more vulnerable to the effects of friendly force weapons, maneuver, and operations.

- **Electronic Warfare**

Electronic warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-51). ... The three major components of EW are electronic protection (EP), electronic warfare support (ES), and electronic attack (EA).

- **Electronic Protection.** *Electronic protection* is that division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability (JP 3-51).
- **Electronic Warfare Support.** *Electronic warfare support* is that division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations.
- **Electronic Attack.** *Electronic attack* is that division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

- **Computer Network Operations**

Computer network operations comprise computer network attack, computer network defense, and related computer network exploitation enabling operations. CNO is not totally applicable at the tactical level. CNO is applicable at echelons above corps.

- 2-31. *Computer network attack* is operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (JP 3-13).
- *Computer network defense* consists of defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction (JP 3-51). It

includes all measures to detect unauthorized network activity and adversary CNA and defend computers and networks against it.

- *Computer network exploitation* consists of enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.

- **Supporting Elements**

The supporting IO elements are physical destruction, IA, physical security, counterintelligence, counterdeception, and counterpropaganda.

- **Physical Destruction**

Physical destruction is the application of combat power to destroy or degrade adversary forces, sources of information, command and control systems, and installations. It includes direct and indirect fires from ground, sea, and air forces. Also included are direct actions by special operations forces.

- **Information Assurance**

Information assurance comprises information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (JP 3-13).

- *Availability* means timely, reliable access to data and services by authorized users. Available INFOSYS operate when needed.
- *Integrity* means protection from unauthorized change, including destruction. INFOSYS with integrity operate correctly, consistently, and accurately.
- *Authentication* means certainty of user or receiver identification and authorization to receive specific categories of information.
- *Confidentiality* means protection from unauthorized disclosure.
- *Nonrepudiation* means proof of message receipt and sender identification, so neither can deny having processed the data.

- **Physical Security**

Physical security is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (JP 3-13). Effective physical security ensures the availability of INFOSYS used to conduct operations.

- **Counterintelligence**

Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 3-13). The CI mission is to detect, identify, assess, counter, neutralize, or exploit hostile intelligence collection.

- **Counterdeception**

Counterdeception consists of efforts to negate, neutralize, diminish the effects of, or gain the advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations (JP 3-13). Counterdeception contributes to situational understanding and defensive IO by protecting friendly C2 systems and decision-makers from adversary deception. Its goal is to make friendly decision-makers aware of adversary deception activities so they can formulate informed and coordinated responses.

- **Counterpropaganda**

Counterpropaganda consists of programs of products and actions designed to nullify propaganda or mitigate its effects (FM 3-05.30). It is directed toward the target of adversary propaganda. Counterpropaganda degrades the harmful influence of adversary PSYOP on friendly forces and other audiences (see JP 3-53; FM 3-05.30; FM 33-1-1). ... Counterpropaganda includes countering adversary misinformation, disinformation, and opposing information.

- **Related Activities**

Related activities include, but are not limited to, [Public Affairs] PA and [Civil Military Operations] CMO.

- **Public Affairs**

Public affairs are those public information, command information, and community relations' activities directed toward both the external and internal publics with interest in the Department of Defense (JP 3-61). (Army doctrine uses the term *internal information* in place of *command information*.) PA information is credible. It makes available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy.

- **Civil Military Operations**

Civil military operations are activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational United States objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government.

Tactics, Techniques, and Procedures

Like all military operations, information operations follow the operations process: planning, preparation, execution, and continuous assessment.

3. Planning Information Operations

- **Information Operations Planning Concepts**

Planning is the means by which the commander envisions a desired outcome, lays out effective ways of achieving it, and communicates to his subordinates his vision, intent, and decisions, focusing on the results he expects to achieve. ... Commanders use the IO mission statement, IO concept of support, IO objectives, and IO tasks to describe and direct IO.

- The *information operations mission statement* is a short paragraph or sentence describing what the commander wants IO to accomplish and the purpose for accomplishing it.
- The *information operations concept of support* is a clear, concise statement of where, when, and how the commander intends to focus the information element of combat power to accomplish the mission.
- *Information operations objectives* are clearly defined, obtainable aims that the commander intends to achieve using IO elements/related activities.
- *Information operations tasks* are tasks developed to support accomplishment of one or more information operations objectives. An IO task addresses only one IO element/related activity.

The most important IO planning product is the IO subparagraph or IO annex of the operation plan (OPLAN) or operation order (OPORD) (see appendix D). The IO annex usually includes an IO execution matrix and IO assessment matrix as appendixes.

- **Receipt of Mission**

Upon receipt of a mission, either from higher headquarters or from the commander, the commander and staff perform an initial assessment. Based on this assessment, the commander issues initial guidance and the staff prepares and issues a WARNO. During the time between receiving the commander's initial guidance and issuing the WARNO, the staff performs [the following] receipt of mission actions:

- Participates in the commander's initial assessment.
- Receives the commander's initial guidance.
- Reviews the IO estimate.
- Prepares for future planning.

- **Mission Analysis**

During mission analysis, the staff defines the tactical problem and begins to determine feasible solutions. Mission analysis consists of 17 tasks. Many of them are performed concurrently. The mission analysis products are the restated mission, initial commander's intent, commander's guidance, and at least one WARNO. ... The staff performs the following tasks during mission analysis:

- Analyze the higher headquarters order.
- Conduct IPB.
- Determine specified, implied, and essential tasks.
- Review available assets.
- Determine constraints.
- Identify critical facts and assumptions.
- Conduct risk assessment.
- Determine initial commander's critical information requirements.
- Determine the initial ISR annex.
- Plan use of available time.

- Write the restated mission.
- Conduct a mission analysis briefing.
- Approve the restated mission.
- Develop the initial commander's intent.
- Issue the commander's guidance.
- Issue a WARNO.
- Review facts and assumptions.

- **Course of Action Development**

After the mission analysis briefing, the staff begins developing COAs for analysis and comparison based on the restated mission, commander's intent, and planning guidance. During COA development, the staff prepares feasible COAs that integrate the effects of all combat power elements to accomplish the mission. Based on the initial IO mission statement, the G-7 develops a distinct IO concept of support, IO objectives, and IO tasks for each COA [while performing the following actions].

- Analyze relative combat power
- Generate options
- Array initial forces
- Develop the concept of operations
- Recommend headquarters [for command and control]
- Prepare COA statements and sketches

- **Course of Action Analysis (War-gaming)**

COA analysis (war-gaming) identifies which COA accomplishes the mission with minimum casualties while best positioning the force to retain the initiative. War-gaming is a disciplined process that staffs use to envision the flow of battle. Its purpose is to stimulate ideas and provide insights that might not otherwise be discovered. Effective war-gaming allows the staff to test each COA, identify its strengths and weaknesses, and alter it if necessary.

- **Course of Action Comparison**

During COA comparison, the staff compares feasible courses of action to identify the one with the highest probability of success against the most likely adversary COA and the most dangerous adversary COA. Each staff section evaluates the advantages and disadvantages of each COA from the staff section's perspective, and presents its findings to the staff. The staff outlines each COA in terms of the evaluation criteria established before the war game and identifies the advantages and disadvantages of each with respect to the others.

- **Course of Action Approval**

After completing the COA comparison, the staff identifies its preferred COA and recommends it to the commander—in a COA decision briefing, if time permits. The concept of operations for the approved COA becomes the concept of operations for the operation itself. The IO concept of support for the approved COA becomes the IO concept of support for the operation. Once a COA is approved, the commander refines the commander's intent and issues additional planning guidance.

- **Orders Production**

Based on the commander's decision and final guidance, the staff refines the approved COA and completes and issues the OPLAN/OPORD. Time permitting, the staff begins planning branches and sequels.

4. Preparing for Information Operations

Preparation for information operations (IO) includes actions performed before execution to improve the ability to conduct both offensive and defensive IO. It includes revising and refining plans and orders, assessment, force protection, coordination and liaison, rehearsals, task organization and movements, preoperation checks and inspections, logistic preparations, and integration of new soldiers and IO-capable units. When a unit executing one mission receives a warning order for a follow-on mission, it begins preparing for that mission while executing its current mission.

5. Executing Information Operations

The complexity of information operations (IO) execution stems from IO's multiple elements with their diverse operational capabilities and requirements. The wide variance in the time IO elements need to achieve effects and the coordination required between echelons add complexity. Well-executed IO results in confused and demoralized adversary leaders and soldiers. It produces psychologically and electronically isolated adversary units incapable of mounting coordinated efforts. Often, adversary commanders are severed from their subordinates and powerless to counter Army force actions at the decisive point. ... [Effective] IO execution {includes}: staff coordination, assessing IO, decision-making, and other IO-related considerations.

~ ~ ~

The current version of FM 3-13, Information Operations (28 Nov 2003), is available on line from the General Dennis J. Reimer Training and Doctrine Digital Library at:

atiam.train.army.mil/soldierPortal/atia/adlsc/view/public/7422-1/fm/3-13/toc.htm

Last Updated: November 2007.

Marine Corps Information Operations Doctrine



Key doctrinal documents:

- Marine Corps Order 3430.8, *Policy for Information Operations*, 19 May 1997
- Marine Corps Order 3432.1, THE MARINE CORPS OPERATIONS SECURITY (OPSEC) PROGRAM
- MCWP 3-40.4, *MAGTF Information Operations*, 9 Jul 2003.
- MCWP 3-40.2, *Information Management*, 24 Jan 2002. (Focuses on defensive measures).
- MCWP 3-40.5, *Electronic Warfare*, 10 Sep 2002.
- MCWP 3-40.6 Psychological Operations (Dual Designated w/ Army)
- MCRP 3-40.6A PSYOP tactics, techniques, and procedures (Dual Designated)
- MCRP 3-40.6B Tactical PSYOP TTP's (Dual Designated w/ Army)

Excerpts of Marine Corps Doctrine - MCWP 3-40.4 (9 Jul 2003)

Information Operations in Support of Expeditionary Warfare

“Marine Corps information operations (IO) support maneuver warfare through actions that use information to deny, degrade, disrupt, destroy or influence an adversary commander’s methods, means or ability to C2 his forces and to inform target audiences through informational activities. IO enhance the ability of the MAGTF to project power during peace and war. They complement and facilitate the traditional use of military force but in some instances may stand alone as a deterrent option. IO support the integration of situational awareness, operational tempo, influence, and power projection to achieve advantage.”

IO is an integrating concept that facilitates the warfighting functions of C2 (command and control), fires, maneuver, logistics, intelligence, and force protection. IO is not simply another “arrow” in the MAGTF commander’s quiver. IO is a broad-based capability that “makes the bow stronger.”

IO is multi-disciplined. Capabilities relevant to IO include, but are not limited to, the five core capabilities of IO, -- psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), electronic warfare (EW), computer network operations (CNO), as well as the supporting and related capabilities. These include public affairs (PA), civil-military operations (CMO), and combat camera (COMCAM). IO conducted by MAGTFs support battlespace shaping, force enhancement, and force protection activities. IO will enhance the ability of the MAGTF to project power during peace and war, complementing and facilitating the traditional use of military force.

MAGTFs will execute IO to enable and enhance their ability to conduct military operations consistent with the Marine Corps’ capstone concept, *Expeditionary Maneuver Warfare (EMW)*. The MAGTF can support joint and multinational enabling by serving as an adaptive cornerstone force-bringing flexible command, control, communications, computers, and intelligence (C4I) systems that allow a joint or

coalition force to be assembled in an expeditionary environment. Marines also bring unique capabilities, such as the electronic attack (EA)-6B Prowler aircraft and the Mobile Electronic Warfare Support System, adding to the combat power of the joint force. The Communications Emitter Sensing and Attack System (CESAS) is taking over some of the EA mission for the Radio Battalions. The MAGTF will frequently rely on national level agencies and other service components for certain offensive and defensive IO related capabilities.

IO can increase strategic agility by utilizing the reach back capability of MAGTF command, control, communications, and computers (C4) systems thus allowing the MAGTF to draw upon information sources outside its area of operations. IO can extend operational reach through informational and media activities that unify power projection with influence projection. IO can increase tactical flexibility by providing the MAGTF commander with a range of both lethal and nonlethal options. Finally, IO can enhance support and sustainment by enabling power projection against distant targets without increasing the MAGTF's footprint ashore.

Principles

- *IO is an integral function of the MAGTF.*
- *MAGTF IO is focused on the objective.*
- *The MAGTF commander's intent and concept of operations determine IO targets and objectives.*
- *MAGTF IO must be synchronized and integrated with those of the higher and adjacent commands*
- *MAGTF IO is supported by the total force.*
- *Many different capabilities and activities must be integrated to achieve a coherent IO strategy.*
- *Intelligence support is critical to the planning, execution, and assessment of IO.*

Offensive and Defensive Operations

- **Offensive IO** objectives must be clearly established. They must support overall national and military objectives and include identifiable indicators of success. Selection and employment of specific offensive capabilities against an enemy must be appropriate to the situation. Offensive IO may be the main effort, a supporting effort or a phase in the MAGTF operation. Offensive IO objectives include the following:
 - Influence the adversary commander's estimate of the situation.
 - Slow the adversary's tempo of operations.
 - Degrade the adversary commander's decision cycle for planning and executing operations.
 - Disrupt the adversary commander's ability to generate and focus combat power.
- **Defensive IO** ensure timely, accurate, and relevant information access while denying the enemy the opportunity to exploit friendly information and information systems for its own purposes. Since it is a practical impossibility to defend every aspect of the infrastructure and every information process, defensive IO provide the essential and necessary protection and defense of information and information systems upon which the MAGTF depends to conduct operations and achieve objectives.

The basis for defensive IO planning is the conduct of OPSEC, C4 vulnerability analysis, identification and protection of essential elements of friendly information, and the generation of the restricted frequency list.

The objectives of defensive IO include the following:

- Sustain the MAGTF commander's freedom of action.
- Reduce the adversary's ability to affect friendly C2.
- Minimize friendly C2 system vulnerabilities to adversary C2 attack through the employment of adequate physical, electronic, information, and OPSEC measures.
- Minimize friendly mutual interference on friendly C2 and unintended third parties throughout the electromagnetic spectrum.
- Minimize the effects of adversary perception management activities.

Operational Focus. The primary focus of MAGTF IO activities will be at the operational and tactical levels of war.

Staff Responsibilities

- The G-3/S-3 is responsible for IO. The future operations section is responsible for overseeing the planning and coordination of the IO effort. The MAGTF IO officer, within G-3/S-3 future operations, is responsible for:
 - The broad integration and synchronization of IO efforts.
 - Responding directly to the G-3/S-3 for MAGTF IO.
 - Ensuring that the IO cell provides input to the operational planning team (OPT) during planning to ensure coordinated operations.
 - Preparing the IO appendix to the operation order (OPORD).
 - Overseeing the core personnel within the IO cell as well as augmentees from external agencies.
 - Ensuring that all IO matters are coordinated within the MAGTF staff, higher headquarters, and external agencies.
- The electronic warfare officer (EWO) integrates EW operations through the EW coordination center or the IO cell when established.

Information Operations Cell

The IO cell is a task-organized group that is established within a MAGTF and/or higher headquarters to integrate a variety of separate disciplines and functions pertaining to IO for the command. A fully functioning IO cell integrates a broad range of potential IO actions and related activities that contribute to accomplishing the mission. IO integration requires extensive planning and coordination among all the elements of the staff. The IO cell, when established, is a mechanism for achieving that coordination.

Information Operations Capabilities

- **Overview.** IO include all action taken to affect enemy information and information systems while defending friendly information and information systems. IO are focused on the adversary's key decision-makers. IO are conducted during all phases of an operation, across the range of military operations, and at every level of war.

Note: The following *descriptions* are presented vice the *definitions* which in most cases are the respective Joint definitions found in JP 1-02.

- **Deception.** Military deception targets enemy decision makers by targeting their intelligence collection, analysis, and dissemination systems. Deception requires a thorough knowledge of adversaries and their decision making processes. Military deception is focused on achieving a desired behavior, not simply to mislead. The purpose is to cause adversaries to form inaccurate impressions

about friendly force capabilities or intentions by feeding inaccurate information through their intelligence collection or information assets. The goal is to cause the adversary to fail to employ combat or support units to their best advantage.

- **Electronic warfare** is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or the attack the enemy. The three major subdivisions within EW are: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). (JP 1-02)
- **Operational Security.** OPSEC is the key to information denial. It gives the commander the capability to identify indicators that can be observed by adversary intelligence systems. These indicators could be interpreted or pieced together to derive critical information regarding friendly force dispositions, intent, and/or COAs that must be protected. The goal of OPSEC is to identify, select, and execute measures that eliminate or reduce indications and other sources of information, which may be exploited by an adversary, to an acceptable level.
- **Psychological Operations** (PSYOP) are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. (JP 1-02). See also MCWP 3-40.6 (formerly FMFM 3-53), *Psychological Operations*....Note: The Marine Corps is standing up a Tactical PSYOP Team (TPT) that will be attached to each Marine Expeditionary Unit (MEU). It will consist of one officer and three enlisted, and concerned solely with tactical PSYOP. If requested, external PSYOP support at echelons higher than the MEU may be provided by the US Army's 4th Psychological Operations Group (POG).
- **Computer Network Operations.** CNO support C2 by facilitating the decision making process by providing communication and information systems that are reliable, secure, timely, and flexible. CNO protect information and information processes through computer network defense and IA activities. CNO may also be used to attack or exploit an adversary's information systems through computer network attack or exploitation. The Marine cryptologic support battalion or the RadBn may be tasked to support CNO activities. While the MAGTF does not have a computer network attack (CNA) force, it must be aware of available joint capabilities. Additionally, the MAGTF must be prepared to defend against the CNA threat posed by the adversary.
- **Physical Attack** applies friendly combat power against the enemy. It reduces enemy combat power by destroying enemy forces, equipment, installations, and networks. Within IO, physical destruction is the tailored application of combat power to achieve desired operational effects.
- **Information Assurance.** IA is information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP-02). IA capabilities include information security.
- **Physical Security** contributes directly to information protection. Information, information-based processes, and information systems—such as C4 systems, weapon systems, and information infrastructures— are protected relative to the value of the information they contain and the risks associated the compromise or loss of information.
- **Counterintelligence.** The principal objective of CI is to assist with protecting friendly forces. CI is the intelligence function concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion or terrorism. CI enhances command security by denying adversaries information that might be used against friendly forces and to provide protection by identifying and neutralizing

espionage, sabotage, subversion or terrorism efforts. CI provides critical intelligence support to command

- **Public Affairs.** The PA mission is to provide timely, accurate information to Marines and the general public and to initiate and support activities contributing to good relations between the Marine Corps and the public. PA expedites the flow of accurate and timely information to internal and external audiences. In peacetime, PA provides Marine and the general public with information that increases public understanding of the Marine Corps' roles and missions. PA efforts can have positive as well as negative impacts within the battlespace and the consequences of its use can have a strategic effect on the mission.
- **Civil-Military Operations.** Each military operation has a civil dimension. The civil dimension requires that commanders consider how their actions affect, and are affected by, the presence of noncombatants. Accordingly, CMO have become an integral element of military operations. Through careful planning, coordination, and execution, CMO can help the MAGTF win by shaping the battlespace, enhancing freedom of action, isolating the enemy, meeting legal and moral obligations to civilians, and providing access to additional capabilities.

Intelligence Support to Planning. Intelligence provides the essential basis for planning IO through the following considerations:

- The adversary commander's freedom of action and the freedom of action allowed to subordinates including adversary perceptions of the situation and developments.
- Adversary IO capability, intent, morale, and vulnerability to offensive IO.
- C2 aspects such as key personnel, target audiences, headquarters, communications nodes, databases or intelligence collection systems. C2 nodes that appear in more than one adversary COA should be highlighted for targeting.
- Assessments of friendly vulnerability to adversary IO.

Similar intelligence products support each of the various IO capabilities; for example, OPSEC, PSYOP, deception, EW, CNO, CI, physical attack, physical security, IA. The intelligence requirements for each capability are interrelated.

Updated: September 2007.

This Page Intentionally Blank

Navy Information Operations Doctrine



Key doctrine and tactics, techniques, and procedures

- NWP 3-13, *Navy Information Operations*, June 2003
- NTTP 3-13.1, *Theater and Campaign Information Operations*, January 2002
- NTTP 3-13.2, *Navy IO Warfare Commander's Manual*, May 2005
- Core Capabilities:
 - NTTP 3-51.1, *Navy Electronic Warfare* (Feb 06)
 - TACMEMO 3-13.2-03, *Psychological Operations for Navy Planners*, October 2003
 - NTTP 3-54.3, *Navy Operations Security*, July 2005
 - NTTP 3-58.1, *Multi-Service Military Deception Planners Guide* (April 2007)
 - NTTP 3-58.2, *Navy Military Deception*, March 2006
 - NTTP 3-51.2, *Multi-Service Reprogramming*, January 2007
 - NWP 3-63, *Navy Computer Network Operations* (draft)
- **Fleet Concept of Operations (CONOPS)**
 - Fleet Information Operations, December 2006
 - Maritime Influence, August 2007 (draft)
 - Maritime Headquarters-Maritime Operations Center (MHQ-MOC), March 2007
 - NNWC Maritime Operations Center (in development)
 - Computer Network Operations (in development)
- **NWPs, NTTPs, TACMEMOs, and CONOPS are available at:** <http://www.nwdc.navy.smil.mil> under the Navy Warfare Library link.

Summary of Navy Information Operations Doctrine and Concepts

Introduction

The United States (U.S.) has experienced a shift from strictly symmetric, or force-on-force, warfare to more asymmetric warfare and military operations. Many of today's adversaries rely primarily on operations such as terrorism, disinformation, and propaganda campaigns to circumvent or undermine U.S. and allied strengths and exploit friendly vulnerabilities. Future Navy forces will continue to face adversaries outside the generally accepted force-on-force environment of the past. Naval forces are challenged by asymmetric operations in all domains—surface, subsurface, air, ground, and cyberspace—and must therefore defend against, defeat, deny, or negate the capabilities that will be used to prevent U.S. freedom of access. Information Operations (IO) is applicable across the range of military operations, (e.g., supporting major combat operations, global war on terrorism, etc.), in support of the Navy operating concept. Furthermore, the Navy must provide IO capabilities, organizational structures, planning processes, and personnel to maritime headquarters (MHQs)/joint force maritime component commanders (JFMCCs) engaged in theater security cooperation plans (TSCPs) and/or combat operations that enable our forces to engage in the asymmetric domain. Rapid advances in information technology provide today's military with unparalleled abilities to collect, process, and disseminate information. Technological

advances have also increased the commander's vulnerability as a target for adversary information collection, shaping, and attack. IO will continue to play a key role by allowing the Navy and its partners to dominate warfare in the maritime domain. Operations within this domain include controlling the sea, conducting operational maneuvers throughout the world, deterring aggression through forward presence and influence operations in peacetime, responding to crisis, conducting major combat operations, and complementing other instruments of national power by projecting power from the sea, directly and decisively influencing events ashore.

Core Capabilities of Information Operations

IO was established as a warfare area within the Navy with the goal of affecting accuracy, usability, timeliness, completeness, or relevance of information used in guiding and conducting operations. IO includes electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC). Supporting capabilities of IO include physical attack, physical security, information assurance, public affairs (PA), combat camera/visual information, civil-military operations, legal affairs, meteorology, intelligence, and oceanography. This is Navy IO at its most fundamental level and could consist of a wide (almost unbounded) array of "weapons," within the core, supporting, and related capabilities above.

IO is an integral part of the Navy planning and targeting process that continues through the range of military operations (see Figure 1). From guiding effects-based planning in the earliest stages to the weaponizing assessment phase of the targeting cycle, IO planners can assist in determining the right mix of maneuver, and kinetic/nonkinetic weapons that will produce the commander's desired effect. In addition to offering nonkinetic options to traditional strike warfare, IO plans often require the use of strike group maneuvers (concentration of forces and presence), kinetic strikes, and special operations warfare to deny, disrupt, destroy, or degrade information systems to attain overall campaign objectives. While each capability of IO includes a specialized planning process and can be applied to military operations individually, their coordinated application maximizes friendly advantages.

Information Operations Fundamentals

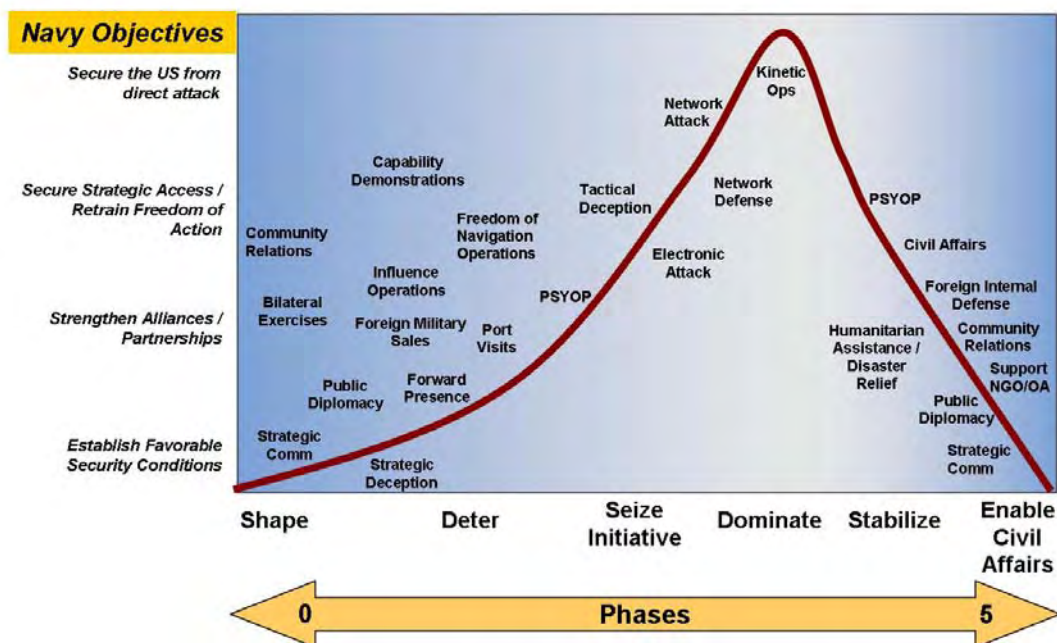


Figure 1. Range of Military Operations Integrating IO

Information Superiority

Information superiority embodies the ability to collect, process, and disseminate the correct information to the right person, at the right place and time, in the right form, while denying an adversary the ability to do the same. Network-centric operations can foster information superiority by networking sensors, decisionmakers, and shooters. The goal of using network-centric operations is to increase mission effectiveness in order to achieve an increased state of readiness. There are five dimensions of information that determine whether or not information is of value to the commander. These are:

- Accuracy - the degree to which the information reflects the actual situation
- Relevance - the degree to which the information is applicable to the situation
- Timeliness - the degree to which the information is available in time to affect the decision
- Usability - the degree to which the information is in a format easily understood by the decision maker
- Completeness - the degree to which all the information required by the decision maker is available.

This superiority contributes to the ability to project maritime power forward from the sea, and ultimately in all warfighting domains. IO supports information superiority by corrupting, deceiving, delaying, denying, disrupting, degrading, or destroying one of the dimensions of information before it is presented to the adversary's commander, while protecting the same friendly information dimensions. Enabled through FORCENet (discussed later), information superiority is achieved through effects-based approach to operations (EBO), maritime power projection, maritime influence, target development, and environmental awareness and shaping (EAS). All echelons and warfare areas strive for and plan to achieve and maintain information superiority through coordinated efforts among the operations, intelligence, and command, control, communications, and computers (C4), and knowledge management.

Effect-Based Approach to Operations

An EBO focuses on improving the commander's ability to affect an adversary's behavior and/or capabilities through the integrated application of select instruments of national power (diplomatic, information, military, economic). Effects are created to achieve objectives and are characterized as the physical and/or behavioral state of political, military, economic, social infrastructure, and information systems. An effects-based approach seeks to develop a commonly shared understanding of the operational environment to provide the commander with a more comprehensive picture of the challenges and the best balance of capabilities to shape the environment. The three main elements within an effects-based approach are as follows:

1. Visualizing the operational environment beyond the traditional military battlespace as an interconnected system-of-systems comprised of friends, adversaries, and the unaligned.
2. Integrating military actions with those of other instruments of national power.
3. Assessing system behaviors and capabilities and effects attainment in addition to task accomplishment.

Maritime Power Projection

No one can predict with certainty the future security environment, but emerging trends require that the Navy focus on littorals and the land beyond. The Navy must remain expeditionary in nature, controlling the sea and moving around the globe to support U.S. national interests. The vision for the future is a Navy and Marine Corps team that will maintain a robust and credible forward presence. These forces provide a framework that complements other instruments of national power to build stability and favorably shape areas overseas. Forward presence, combined with knowledge superiority within the environment, will achieve the ultimate objective—maritime power projection—projecting U.S. power and influence from the sea, directly and decisively influencing events ashore.

Maritime Influence

Naval forces deployed or stationed in areas overseas demonstrate our national resolve, strengthen alliances, and dissuade potential adversaries. IO provides significant support to maritime influence operations during the phases of planning and assessment. U.S. naval forces will protect and use information to influence adversaries, advance friendly objectives, and shape the operating environment to our advantage. With EBO, maritime influence coordinates the employment of maritime activities to affect the attitudes and behaviors of an intended audience in support of commander objectives. With the goal of advancing U.S. interests, maritime influence activities may include actions to deter adversaries, reassuring allies and friends, sending signals of U.S. interest, and fostering good will.

Target Development

Warfighters win engagements and wars when the adversary makes a decision—based on knowledge derived from true or perceived information—to surrender due to an inability to obtain desired objectives. A comprehensive assessment of the adversaries and friendly abilities and functions within the operational environment provide the first step into developing targets. Friendly forces design all campaign plans to influence the adversary to make such a decision. The people and systems that comprise the information grids filter and process the information upon which the commander bases decisions and therefore require defending as part of IO planning. Target development includes nodes that have an impact on the adversary decision making process, which may include command and control systems, communications and weapon systems, and other situation awareness tools.

Environment Awareness and Shaping

EAS describes the functions performed by organizations to ensure that, despite the wide range of nonlethal and lethal means at the disposal of adversaries or potential adversaries, friendly forces are consistently capable of conducting decisive operations and achieving desired results at a minimal loss to friendly forces. The commander uses EAS to identify, protect, and leverage critical information systems, emissions, transmissions, and operational indicators, to achieve and maintain information superiority. Environment awareness equates to knowledge of the operational environment. This knowledge, resulting from the fusion of key elements of information, allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish requirements and priorities, and exploit emerging opportunities, while mitigating the impact of unexpected adversary actions. Environment shaping is the conscious action of molding the environment to prevent conflicts or placing U.S. interests in a favorable position. It involves the continual process of developing, evaluating, and revising the force operational profile within the environment, providing all warfare commanders with critical planning and execution support to ensure that missions are conducted with the least risk to friendly assets.

FORCEnet

FORCEnet provides the operational construct and architectural framework for achieving information superiority by integrating warriors, sensors, networks, command and control, platforms and weapons into a distributed force. FORCEnet provides naval forces with increased operational awareness, while supporting maritime power projection, ensuring access to the littoral areas and deterring conflict through the employment of a network of sensors and communication devices that provide the Navy with real time, shared awareness in support of operational objectives. Networked distributed forces allow warriors to apply speed in information gathering and sharing, and the ability to convert information into knowledge, command, and timely application of effects.

Information Operations Organization Structure

- **Naval Network Warfare Command**

Naval Network Warfare Command (NAVNETWARCOM) provides the Navy's central operational authority and type commander for IO in support of naval forces afloat and ashore. NAVNETWARCOM maintains responsibility for identifying, coordinating, and assessing the Navy's IO requirements and FORCEnet architecture development. As the functional component for IO under U.S. Strategic Command, NAVNETWARCOM is responsible for the Navy's strategic IO planning and operational support.

- **Navy Information Operations Command Norfolk**

Navy Information Operations Command (NIOC) Norfolk, the Navy's Center of Excellence for IO, is responsible for providing operationally focused training; planning support and augmentation from the tactical to the strategic level; developing IO doctrine, tactics, techniques, and procedures; advocating requirements in support of future effects-based warfare; conducting experimentation for evaluating emerging or existing IO technologies and doctrine; providing and managing IO data for fleet operations. NIOC Norfolk operates under the operational and administrative control of NAVNETWARCOM, and has two subordinate commands: NIOC San Diego and NIOC Whidbey Island.

- **Navy Cyber Defense Operations Command**

The Navy Cyber Defense Operations Command (NCDOC) (formerly NAVCIRT), coordinates, monitors, and oversees the defense of Navy computer networks and systems, including telecommunications, and is responsible for accomplishing computer network defense (CND) missions as assigned by NAVNETWARCOM and Joint Task Force - Global Network Operations (JTF-GNO).

- **Navy Information Operations Command Suitland**

Navy Information Operations Command (NIOC) Suitland serves as Navy's IO innovation center and functions as the principal technical agent for research and development of prototype IO capabilities. NIOC Suitland supports the development capabilities encompassing all aspects of IO attack, protect, and exploit; maintaining an aggressive program to acquire and analyze state-of-the-art technologies (software and hardware), evaluate fleet applicability, and prototype developmental capabilities. NIOC Suitland maintains a collaborative relationship with Space and Naval Warfare Systems Command, Systems Center San Diego to provide efficient and effective technical expertise in command, control, communications, computers, intelligence, surveillance, reconnaissance and information operations. NIOC Suitland also supports development coordination between NAVNETWARCOM, OPNAV, NIOC Norfolk, systems commands, IO technology center, and the commercial industry.

Navy Information Operations Employment Concept

Sea Power 21 describes future naval operations that will use information superiority and dispersed, networked force capabilities to deliver effective offensive power, defensive assurance, and operational independence to joint force commanders. To support Sea Power 21, the Navy's focus is to integrate and align IO to support all levels of operations:

- At the strategic level, national leadership and regional commanders will use IO to achieve national/theater shaping and influencing objectives. Regional commanders will integrate Navy IO capabilities with other services, other U.S. government departments and agencies, and partner nations as part of their theater security cooperation plans (TSCP). At this level, IO is a key element of EBO.

- At the operational level, IO supports campaign/major operational objectives by providing information superiority through shaping and controlling the information environment. At this level, the focus of IO is control of adversary lines of communication (logistics information, command and control, and related capabilities and activities) while protecting the friendly information environment.
- At the tactical level, Navy IO will make full use of the core capabilities to dominate the information environment for the commander. At this level, IO will be used to tactically influence adversaries or deny, destroy, or degrade systems critical to the adversary's conduct of operations.

Levels of Operations	Key Goals Include...	Objectives to Support Goals Include...	Application of Navy IO Include...	Impact of Navy IO...
Strategic (National and Theater) National Security Strategy National Guidance & Military Strategy Theater Strategy & Campaign Plans	Implementation of long-term national and theater shaping, and theater security cooperation plans (TSCPs).	Influence nations/potential adversaries/decision makers globally or in a specific region(s). Support diplomacy, stabilize regions, and assure allies. Deter war. Support intelligence preparation of the environment, and shape environment to U.S. advantage.	CCDR, NCC/MHQ, and JFMCC (when assigned), will use IO to support TSCPs through presence, coordination with public affairs, port calls, multinational exercises, peace operations, and support to strategic communications.	Demonstrate that the U.S. is engaged in the region and can project power. Demonstrate that the U.S. military can project power anywhere in region. Prepare intelligence baseline for future ops. Shape positive perception of U.S. actions.
Operational Subordinate Campaign Plans Major Operations	Decisively defeat adversary ability to control forces.	Shape and control information environment. Use spectrum of IO core capabilities to conduct (or support) force application, deny adversary intelligence, surveillance, reconnaissance (ISR) and command, control, communications, computers (C4). Support information superiority. Protect friendly information environment and physical domain.	The NCC/MHQ and JFMCC use IO in continuing strategic roles plus applying Navy IO capabilities and weapons to engage adversary C4 and ISR and PSYOP to influence adversary forces and populations. Directly support conduct of joint or maritime operations/power projection.	Support information superiority for the joint force commander. Control information environment and physical domain by influencing, disrupting, or corrupting adversarial human and automated decisionmaking.
Tactical Operational Orders and OPTASKS Battles Engagements	Strike Group commander effectively using forces to achieve commander's assigned tasks. Coordinated use of EW, PSYOP, MILDEC, CNO, OPSEC capabilities embedded in Navy forces.	Control tactical information environment and physical domain. Disrupt adversary operations. Undermine adversary ability and will to fight. Disrupt adversary C4, ISR and defensive systems. Protect the naval/joint battle force.	During initial phases of a campaign, Navy strike groups may have the preponderance of tactical IO assets. Strike Group commander via the IO warfare commander will use IO to support NCC and JFMCC objectives, and other tactical operations.	Achieve/maintain decision superiority, control tactical information environment and physical domains, achieves operational objectives of the JFMCC and tactical objectives of the strike group commander.

Figure 2. Operational Model

The following key organizational concepts are being implemented to affect the operational model summarized in Figure 2:

- **Joint Force Maritime Component Commander Level – IO Cell**

Reference: JFMCC Tactical Memoranda (TACMEMO) 3-32-03

The JFMCC IO Cell contributes to the shaping of the environment to enable tactical units to successfully execute assigned tasks. The IO Cell coordinates with the other JFMCC staff cells (i.e. horizontally) and with the IO cells of the other components and other government agencies through the joint force

commander's IO staff (i.e. vertically). The IO cell works with elements of both the current operations cell, the future operations (FOPS) cell, and the Plans cell. Emphasis has been placed on the flexibility and scalability of Navy *maritime headquarters* (MHQs) with *maritime operations centers* (MOC) designed to perform normal and routine operations. Fleet commanders will establish global MHQ-MOC's to serve geographic areas of responsibility, and may have additional JFMCC responsibilities.

- **MHQ-MOC**

The MHQ-MOC performs the fleet management and command and control (C2) role at the Navy operational-level of command across the range of military operations (ROMO). More importantly, the MHQ-MOC performs the roles of planning, directing, monitoring and assessing the integration and synchronization of Joint Maritime Force operational missions as outlined in the Navy operating concept. The MHQ-MOC organizes staff roles and responsibilities by integrating warfighting functions (C2, intelligence, movement and maneuver, fires, sustainment, and protection) across staff functions. Thus, the assessment and long range planning functions are joined in a future plans center and short term planning is performed in the future operations and current operations cells of the operations center. A MHQ-MOC is able to integrate staff actions horizontally and vertically, simultaneously conducting service and joint operations through the MOC and the fleet management functions by leveraging specialized fleet management staff elements. The MHQ-MOC has the capability to fulfill various roles including Commander, Joint Task Force (CJTF), Joint Force Maritime component commander (JFMCC), naval component commander (NCC), and naval component commander in support of combatant commander (NCC CCDR). Both the MOC and fleet management elements of the staff are supported by a third component consisting of shared support elements that provide personnel, processes, and systems that affect operations and fleet management functions. The MOC is an evolving concept, emerging from the Commander, U.S. Fleet Forces Command (COMUSFLTFORCOM) approved CONOPS dated 13 March 2007.

- **Strike Group Level - The IO Warfare Commander (IWC)**

The IO warfare commander (IWC) assigned to each strike group is responsible for the protection of assigned forces against hostile information, information systems, and electronic attacks, as well as hostile propaganda and deceptive techniques. The IWC maintains the tactical IO picture and is responsible to the force commander for establishing force posture for emissions control (EMCON), information conditions (INFOCON), spectrum management, and maintaining a favorable tactical situation (TACSIT). The IWC supports all force plans and evolutions, while coordinating with theater and joint task force (JTF) IO planners.

- **Shore Support – NAVNETWARCOM Maritime Operations Center**

NAVNETWARCOM has established a tailored MOC to provide effective C2 of assigned forces and continuous situational awareness across the components of space, information, and network operations. Intelligence and logistics capabilities will be fully integrated in the MOC to enable and enhance other regional MHQ's ability to assess, plan, and execute operational-level missions, including strategic communications, theater security cooperation, maritime influence, intelligence preparation of the environment, and maritime security operations. Fleet IO centers (FIOC's) provide geographically-focused IO support to regional MHQ-MOC planners. Further, because the MHQ-MOC concept is new and not fully institutionalized in Navy operations or training, there is a dearth of knowledge regarding key elements critical to NAVNETWARCOM's mission, evolution and maturation as a critical operational node.

Last Updated: October 2007.

This Page Intentionally Blank

Air Force Information Operations Doctrine



Key doctrinal documents:

AFDD 2–5, *Information Operations*, 11 January 2005

AFDD 2–5.1, *Electronic Warfare Operations*, 5 November 2002

AFDD 2–5.3, *Public Affairs Operations*, 24 June 2005

AFDDs are available at: <https://www.doctrine.af.mil/> and <http://afpubs.hq.af.mil>.

Information below is valid as of November 2007. However, at the time of printing the Information Operations Primer for AY 08, the process is now taking place which may result in some Air Force Information Operations doctrinal changes. This section reflects the currently published doctrine.

Excerpts of Air Force Doctrine - AFDD 2-5

Forward

The Air Force recognizes the importance of gaining a superior information advantage—an advantage obtained through information operations (IO) fully integrated with air and space operations. Today, gaining and maintaining information superiority are critical tasks for commanders and vital elements of fully integrated kinetic and nonkinetic effects-based operations. Information operations are conducted across the range of military operations, from peace to war to reconstitution. To achieve information superiority, our understanding and practice of information operations have undergone a doctrinal evolution that streamlines the focus of IO to improve the focus on warfighting.

The new framework of information operations groups the capabilities of influence operations, electronic warfare operations, and network warfare operations according to effects achieved at the operational level. Each of these capabilities consists of separate and distinct subcapabilities that, when combined and integrated, can achieve effects greater than any single capability. Integrated Control Enablers (ICE) is a new term used to define what was formerly expressed as information-in-warfare, or IIW. As our understanding of IO has advanced we have come to see that ICE are not IO, but rather the “gain and exploit” capabilities that are critical to all air, space, and information operations. This new framework reflects the interactive relationship found between the defend/attack and the gain/exploit capabilities in today’s Air Force.

Foundational Doctrine Statements

Foundational doctrine statements are the basic principles and beliefs upon which AFDDs are built.

- Information operations (IO) are integral to all Air Force operations and may support, or be supported by, air and space operations.
- The thorough integration of kinetic and nonkinetic air, space, and information capabilities provides the Air Force with a comprehensive set of tools to meet military threats.
- The Air Force defines information superiority as the degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.
- Decision superiority is about improving our capability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. Decision superiority is a relationship between adversary and friendly OODA loop processes.
- The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects. Effective IO depends on current, accurate, and specialized integrated control enablers (ICE) to provide information from all available sources.
- Information operations conducted at the operational and tactical levels may be capable of creating effects at the strategic level and may require coordination with other national agencies.
- IO should be seamlessly integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide, but there should not be a separate IO campaign plan.
- IO applications span the spectrum of warfare with many of the IO capabilities applied outside of traditional conflict. IO may offer the greatest leverage in peace, pre-conflict, transition-to-conflict, and reconstitution.
- Air Force IO may be employed in non-crisis support or military operations other than war (MOOTW) such as humanitarian relief operations (HUMRO), noncombatant evacuation operations (NEO), or counterdrug support missions where Air Force elements are subject to asymmetric threats that could hinder operations or place forces at risk.
- IO presents additional challenges in effects-based planning as there are many variables. Many of these variables have human dimensions that are difficult to measure, may not be directly observable, and may also be difficult to acquire feedback.

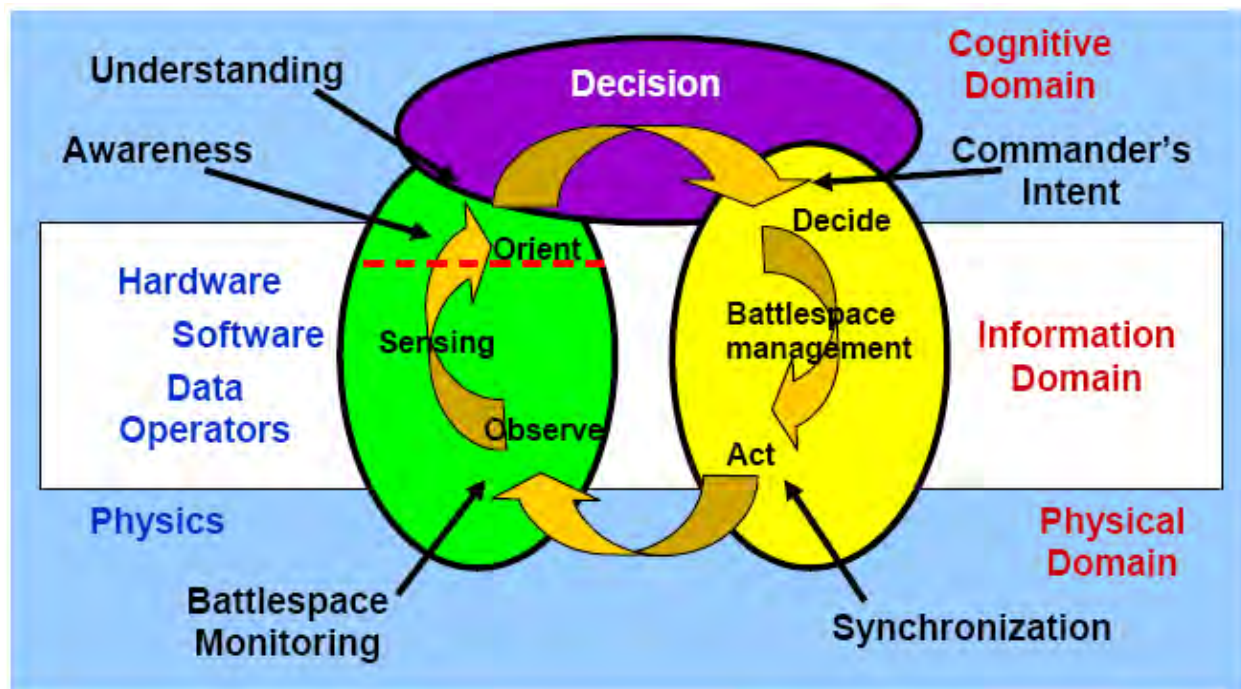
1. The Nature of Information Operations

General Information operations (IO) are the integrated employment of the capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. Information operations provide predominantly nonkinetic capabilities to the warfighter. These capabilities can create effects across the entire battlespace and are conducted across the spectrum of conflict from peace to war and back to peace. Information superiority is a degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. Information superiority is a critical part of air and space superiority, which gives the commander freedom from attack, freedom to maneuver, and freedom to attack. Information operations (IO) are integral to all Air Force operations and may support, or be supported by, air and space operations. IO, therefore, must be integrated into air and space component operations in the same manner as traditional air and space capabilities.

Warfare in the Information Age Warfare in the information age has placed greater emphasis on influencing political and military leaders, as well as populations, to resolve conflict. Information technology (IT) has increased access to the means to directly influence the populations and its leaders. IT has distributed the process of collection, storage, dissemination, and processing of information. The Air

Force goal is to leverage this technology to achieve air, space, and information superiority and to be able to operate in a faster decision cycle (decision superiority) than the adversary. Decision superiority is a competitive advantage, enabled by an ongoing situational awareness, that allows commanders and their forces to make better-informed decisions and implement them faster than their adversaries can react. Decision superiority is about improving our ability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. *Joint Vision 2020* describes it as “better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.” Decision superiority is a relationship between adversary and friendly OODA loop processes. Decision superiority is more likely to be achieved if we plan and protect our OODA loop processes in conjunction with analyzing, influencing, and attacking the adversary’s.

The Information Environment [The information environment can be modeled as the interaction of the physical, information, and cognitive domains as shown below.]



This model provides a means to understand the IO environment. It also provides a logical foundation for the IO capabilities of influence operations, network warfare operations, and electronic warfare operations. All activities in the physical environment have effects in the cognitive environment. Electronic warfare operates in the electromagnetic spectrum, although it creates effects across the range of the IO operating environment. Network warfare operations are focused on the information domain, which is composed of a dynamic combination of hardware, software, data, and human components. Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. The means of influencing can be physical, informational, or both. The cognitive domain is composed of separate minds and personalities and is influenced by societal norms, thus the cognitive domain is neither homogeneous nor continuous.

Societies and militaries are striving to network this “information domain” with the objective of shortening the time it takes for this distributed observe, orient, decide, and act process to occur. It also allows us to automate certain decision processes and to build multiple decision models operating simultaneously. In essence, the information domain continues to expand. New technology increases our society’s ability to transfer information as well as an adversary’s opportunity to affect that information. Information operations are not focused on making decision loops work; IO focuses on defending our decision loops

and influencing or affecting the adversary's decisions loops. This integration of influence, network warfare, and electronic warfare operations to create effects on OODA loops is the unifying theme of IO. Whether the target is national leadership, military C2, or an automated industrial process, how the OODA process is implemented provides both opportunities and vulnerabilities.

The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects. In addition, effective IO depends on current, accurate, and specialized integrated control enablers (ICE) to provide information from all available sources. The thorough integration of kinetic and nonkinetic air, space, and information capabilities provides the Air Force with a comprehensive set of tools to meet military threats.

Influence Operations Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary's decision cycle, which aligns with the commander's objectives. The military capabilities of influence operations are psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, counterpropaganda operations and public affairs (PA) operations. Public affairs, while a component of influence operations, is predicated on its ability to project truthful information to a variety of audiences.

Network Warfare Operations Network warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace. Network warfare operations are conducted in the information domain through the combination of hardware, software, data, and human interaction. Networks in this context are defined as any collection of systems transmitting information. Examples include, but are not limited to, radio nets, satellite links, tactical digital information links (TADIL), telemetry, digital track files, telecommunications, and wireless communications networks and systems. The operational activities of network warfare operations are network attack (NetA), network defense (NetD) and network warfare support (NS).

Electronic Warfare Operations Electronic warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. Electronic warfare operates across the electromagnetic spectrum, including radio, visible, infrared, microwave, directed energy, and all other frequencies. It is responsible for coordination and deconfliction of all friendly uses of the spectrum (air, land, sea, and space) as well as attacking and denying enemy uses. For this reason it is a historically important coordinating element in all operations, especially as current and future friendly uses of the electromagnetic spectrum multiply. The military capabilities of electronic warfare operations are electronic attack, electronic protection, and electronic warfare support.

Integrated Control Enablers Information operations, like air and space operations, are reliant on the integrated control enablers (ICE). ICE includes intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT). Information operations are highly dynamic and maneuverable. The transition between the find, fix, track, target, engage, and assess (F2T2EA) phases can be nearly instantaneous. The ICE components support this interactive relationship and strive to provide commanders continuous decision-quality information to successfully employ information operations.

2 – Influence Operations

General Influence operations are employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the

cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives. They should influence adversary decision-making, communicate the military perspective, manage perceptions, and promote behaviors conducive to friendly objectives. Counterpropaganda operations, psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, and public affairs (PA) operations are the military capabilities of influence operations. They support the commander's objectives and support the Air Force in achieving air, space, and information superiority. This is accomplished by conveying selected information and indicators to target audiences; shaping the perceptions of target decision-makers; securing critical friendly information; protecting against espionage, sabotage, and other intelligence gathering activities; and communicating unclassified information about friendly activities to the global audience.

Psychological Operations Focused on the cognitive domain of the battlespace, PSYOP targets the mind of the adversary. In general, PSYOP seeks to induce, influence, or reinforce the perceptions, attitudes, reasoning, and behavior of foreign leaders, groups, and organizations in a manner favorable to friendly national and military objectives. PSYOP supports these objectives through the calculated use of air, space, and IO with special emphasis on psychological effects-based targeting.

Military Deception Military deception (MILDEC) capabilities are a powerful tool in military operations and should be considered throughout the operational planning process. Military deception misleads or manages the perception of adversaries, causing them to act in accordance with friendly objectives.

Operations Security Operations security (OPSEC) is an activity that helps prevent our adversaries from gaining and exploiting critical information. 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 the adversary. Critical information consists of information and indicators that are sensitive, but unclassified. OPSEC aims to identify any unclassified activity or information that, when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities.

Counterintelligence The Air Force Office of Special Investigations (AFOSI) initiates, conducts, and/or oversees all Air Force counterintelligence (CI) investigations, activities, operations, collections, and other related CI capabilities. Counterintelligence is defined as information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. AFOSI supports influence operations through CI operations designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, manipulation, deception, or repression of the adversary.

Public Affairs Operations Commanders conduct PA operations to assess the information environment in areas such as public opinion and to recognize political, social, and cultural shifts. Public affairs operations are a key component of informational flexible deterrent options and build commanders' predictive awareness of the international public information environment and the means to use information to take offensive and preemptive defensive actions in Air Force operations. Public affairs operations are the lead activity and the first line of defense against adversary propaganda and disinformation. Falsehoods are easily identified when the truth is well known. [Public affairs operations are accomplished through] four core tasks: media operations, internal information, community relations, and strategic communication planning.

Counterpropaganda Operations The Air Force defines counterpropaganda operations as activities to identify and counter adversary propaganda and expose adversary attempts to influence friendly populations and military forces situational understanding. They involve those efforts to negate, neutralize, diminish the effects of, or gain an advantage from foreign psychological operations or propaganda efforts.

Supporting Activities Influence operations are most successful through the seamless integration of kinetic and nonkinetic capabilities. Influence operations may be supported and enhanced by physical attack to create or alter adversary perceptions. Influence operations require support from many Air Force capabilities to include tailored ISR, combat camera operations, and cultural expertise.

3 – Network Warfare Operations

Network warfare operations (NW Ops) are the integration of the military capabilities of network attack (NetA), network defense (NetD), and network warfare support (NS). The integrated planning and employment of network warfare operations along with electronic warfare operations (EW Ops), influence operations, and other military capabilities are conducted to achieve desired effects across the information domain.

Network Attack Network attack (NetA) is employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephony and data services networks. Additionally, NetA can be used to deny, delay, or degrade information resident in networks, processes dependent on those networks, or the networks themselves. A primary effect is to influence the adversary commander's decisions.

Network Defense Network defense (NetD) is employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt, or usurp it. NetD can be viewed as planning, directing, and executing actions to prevent unauthorized activity in defense of Air Force information systems and networks and for planning, directing, and executing responses to recover from unauthorized activity should it occur.

Network Warfare Support Network warfare support (NS) is the collection and production of network related data for immediate decisions involving NW Ops. NS is critical to NetA and NetD actions to find, fix, track, and assess both adversaries and friendly sources of access and vulnerability for the purpose of immediate defense, threat prediction and recognition, targeting, access and technique development, planning, and execution in NW Ops.

4 – Electronic Warfare Operations

General Electronic warfare (EW) is any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack an adversary. The Air Force describes electronic warfare operations (EW Ops) as the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. The EW spectrum is not merely limited to radio frequencies but also includes optical and infrared regions as well. EW assists air and space forces to gain access and operate without prohibitive interference from adversary systems, and actively destroys, degrades, or denies opponents' capabilities, which would otherwise grant them operational benefits from the use of the electromagnetic spectrum.

Electronic Warfare Operations EW is a key contributor to air superiority, space superiority, and information superiority. The most important aspect of the relationship of EW to air, space, and information operations is that EW enhances and supports all operations throughout the full spectrum of conflict. Air Force EW resources and assets may take on new roles in support of operations as the electronic warfare operation mission evolves. The three military capabilities of EW operations are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). All three contribute to air and space operations, including the integrated IO effort. Control of the electromagnetic spectrum is gained by protecting friendly systems and countering adversary systems.

Electronic attack (EA) is the division involving the use of electromagnetic, directed energy (DE), or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of deceiving, disrupting,

denying, and/or destroying adversary combat capability. It also deceives and disrupts the enemy integrated air defense system (IADS) and communications, as well as enables the destruction of these adversary capabilities via lethal strike assets.

Electronic protection (EP) enhances the use of the electronic spectrum for friendly forces. Electronic protection is primarily the defensive aspect of EW that is focused on protecting personnel, facilities, and equipment from any effects of friendly or adversary employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

Electronic warfare support (ES), the collection of electromagnetic data for immediate tactical applications (e.g., threat avoidance, route selection, targeting, or homing) provides information required for timely decisions involving electronic warfare operations.

5 – Information Operations Planning and Execution

Information operations are integral to military operations and are a prerequisite for information superiority. IO supports, and may also be supported by, air and space operations and needs to be planned and executed just like air operations. IO should be seamlessly integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide, but there should not be a separate IO campaign plan.

One of the commander's priorities is to achieve decision superiority over an adversary by gaining information superiority and controlling the information environment. This goal does not in any way diminish the commander's need to achieve air and space superiority but rather facilitates efforts in those areas and vice versa. The aim of information superiority is to have greater situational awareness and control than the adversary. Effective use of IO leads to information superiority. The effort to achieve information superiority depends upon two fundamental components: an effects-based approach, and well-integrated IO planning and execution accomplished by IO organizations.

Effects-Based Approach The ability to create the effects necessary to achieve campaign objectives, whether at the strategic, operational, or tactical levels, is fundamental to the success of the Air Force. An effect is the anticipated outcome or consequence that results from a particular military operation. The emphasis on effects is as crucial for successful IO as for any other air and space power function. Commanders should clearly articulate the objectives or goals of a given military operation. Effects should then flow from objectives as a product of the military operations designed to help achieve those objectives. Based on clear objectives, planners should design specific operations to achieve a desired outcome, and then identify the optimum capability for achieving that outcome. It is important to realize that operational assessment may be more challenging in IO because the effects are often difficult to measure. IO may also be based upon common sense, a rule of thumb, simplification, or an educated guess that reduces or limits the search for solutions in domains that are difficult or poorly understood. For example, psychological effects are not only difficult to measure; they may also not manifest themselves until later in time. There are also second-order and third-order effects that should be taken into consideration, and again, these may not manifest themselves until much later. IO presents additional challenges in effects-based planning as there are many variables. Many of these variables also have human dimensions that are difficult to measure, may not be directly observable, and may also be difficult to acquire feedback. At all times, objectives must be set and effects must be analyzed from the point of view of the culture where operations are being conducted.

Information Operations Organizations A number of Air Force organizations contribute to effective IO. The following discuss several of the key organizations employed in information operations.

Information Warfare Flight (IWF) IO can be conducted throughout the spectrum of peace and conflict. In peacetime, the major command/ numbered air force (MAJCOM/NAF) IWF is the operational planning element for IO and may coordinate IO actions when an air and space operations center (AOC) has not

been activated. When the AOC is activated, a portion of the IWF is established as an IO team and integrates into the warfighting divisions within the AOC (Strategy, Plans, ISR, Combat Operations, etc.). The IO team provides the IO expertise to plan, employ, and assess IO capabilities prior to the initiation of hostilities, transition to conflict, and reconstitution.

EW Ops Organizations Electronic warfare is conducted by units with capabilities ranging across the electronic attack, protect, and support functions. EW operations require attention before, during, and after military operations. A joint EW coordination cell (EWCC) is the necessary planning and execution organization to orchestrate the activities of units to achieve EW objectives of the campaign plan.

Network Defense and Network Operations Organizations NetD and NetOps organizations provide the JFC with critical capabilities to realize the effects of information and decision superiority. Collectively, these organizations provide varying degrees of NetD and NetOps support. They provide commanders with real-time intrusion detection and perimeter defense capabilities, network management and fault resolution activities, data fusion, assessment, and decisions support. During employment, the organizations are arranged into a three-tiered operational hierarchy, which facilitates synchronized application of their collective capabilities in support of the DOD's defense-in-depth security strategy.

6 – Integrated Control Enablers

Information operations are dependent on [integrated control enablers] (ICE). The integrated control enablers are critical capabilities required to execute successful air, space, and information operations and produce integrated effects for the joint fight. These include intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT).

Network Operations and Information Assurance NetOps encompasses information assurance (IA), system and network management, and information dissemination management. The Air Force and joint community have come to recognize these pillars as information assurance and network defense, enterprise service management/network management, and content staging/information dissemination management respectively. NetOps consists of organizations, procedures, and functionalities required to plan, administer, and monitor Air Force networks in support of operations and also to respond to threats, outages, and other operational impacts.

Information assurance (IA) comprises those measures taken to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation (ability to prove sender's identity and prove delivery to recipient). IA spans the full lifecycle of information and information systems. IA depends on the continuous integration of trained personnel, operational and technical capabilities, and necessary policies and procedures to guarantee continuous and dependable information, while providing the means to efficiently reconstitute these vital services following disruptions of any kind, whether from an attack, natural disaster, equipment failure, or operator error. In an assured information environment, warfighters can leverage the power of the information age.

Intelligence, Surveillance, and Reconnaissance ISR is the integrated capabilities to task, collect, process, exploit, and disseminate accurate and timely intelligence information. ISR is a critical function that helps provide the commander the situational and battlespace awareness necessary to successfully plan and conduct operations. Commanders use the intelligence information derived from ISR assets to maximize their own forces' effectiveness by optimizing friendly force strengths, exploiting adversary weaknesses, and countering adversary strengths.

Predictive Battlespace Awareness Effective IO depends upon a successful PBA. As a maturing concept, PBA is "knowledge of the operational environment that allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions" (Air Force

Pamphlet 14-118). In order to accomplish this, PBA lays out a methodology that enables integration of all intelligence, surveillance, and reconnaissance assets available to commanders, in order to maximize their ability to predict enemy courses of action and decide friendly courses of action. One of the first steps in PBA is assessing friendly vulnerabilities and adversary strengths and weaknesses in order to predict enemy courses of action through IPB. This level of awareness requires development and integration of five key activities: IPB, target development, ISR strategy and planning, ISR employment, and assessment. These activities are continuously refined in parallel to provide a seamless understanding of the battlespace.

Precision Navigation and Timing Precision navigation and timing (PNT) provided by space-based systems are essential to IO by providing the ability to integrate and coordinate IO force application to create effects across the battlespace.

7 – Education and Training

Education and training provide the foundation for conducting effective information operations. All Airmen should have a general understanding of information operations capabilities. As in other specialties, IO personnel should be thoroughly trained in the specific IO processes that relate to their particular field of expertise. IO personnel should recognize the contribution their functional specialty makes to the warfighter to help achieve the goal of information superiority. The intent of IO education and training is to ensure Air Force IO operators clearly understand the principles, concepts, and characteristics of information operations. Finally, while not every Airman needs a comprehensive course in information operations, every Airman should understand that IO is a key function of the Air Force distinctive capabilities of information superiority and air and space superiority.

Note: End of AFDD 2-5 extract.

Last Updated: November 2007

This Page Intentionally Blank

Service Component Information Operations Organizations



This Page Intentionally Blank

Army – 1st Information Operations Command (1st IO Cmd)



Mission: 1st Information Operations (IO) Command (Land) provides IO support to the Army and other Military Forces through deployable IO support teams, IO reachback planning and analysis, and the synchronization and conduct of Army Computer Network Operations (CNO) in coordination with other CNO and Network Operations stakeholders, to operationally integrate IO, reinforce forward IO capabilities, and to defend Cyberspace in order to enable IO throughout the Information Environment.

Tasks:

1. Organize, train, equip and deploy mission capable IO Support Teams to provide IO planning and execution support or to conduct IO assessments as directed.
2. Provide IO planning plus operational, technical, and intelligence analysis reachback support to deployed IO support teams and supported commands.
3. Provide IO training support to LCCs, Army Commands, other Service Commands, Joint Forces, Agencies and Activities, as directed
4. Execute the Army Reprogramming Analysis Team-Threat Analysis program.
5. Develop and promote processes and procedures to ensure IO interoperability with Joint Forces, other Services, Inter-agencies, and Allies.
6. Provide IO support for the assessment of force readiness and capabilities of Land Component Forces to accomplish their assigned missions as directed.
7. Synchronize and conduct Army Computer Network Operations (CNO) in coordination with CNO and NETOPS stakeholders to defend Cyberspace and to enable other Information Operations as directed.
8. Operate and maintain the Army's Operations Security (OPSEC) Support Element.
9. Act as the Functional Proponent for Military Deception.

As the single Army organization wholly dedicated to IO, 1st IO Cmd is responsible for providing IO support to the warfighter in planning, synchronizing, de-conflicting, executing, and assessing IO effects for worldwide Army warfighting and other commanders in conflict, other contingency operations, in garrison, and in field training exercises and experiments. 1st IO Cmd operates with and across each of the IO competencies to gain an advantage through coordinated use of multiple capabilities to affect the Information Environment. 1st IO Cmd deploys IO Support Teams that provide IO planning, vulnerability

assessments, OPSEC awareness, training for single and multi-disciplined IO, and technical support for computer incidents and intrusions. 1st IO Cmd conducts and synchronizes operations across the computer network operations (CNO) spectrum in the defense of Army networks by conducting continuous Computer Network Defense (CND) operations and CND-Response Actions in coordination with computer network service providers. Additionally, 1st IO Cmd provides IO reachback capability to deployed teams and to the operational and tactical staffs of deployed forces, as directed. Lastly, 1st IO Cmd executes the Army Reprogramming Analysis Team-Threat Analysis program to enhance the survivability and lethality of warfighting systems. These skilled professionals offer commanders nontraditional options for today's technologically advanced battlespace.

Subordination: 1st IO Cmd is a major subordinate unit to the U.S. Army Intelligence and Security Command (INSCOM) but is under the Operational Control and tasking of the Army G-3 (Director of Operations, Readiness and Mobilization).

Leadership: The Commander of 1st IO Cmd is an Army Colonel (O-6).

Location: The 1st IO Cmd is located at Ft. Belvoir, VA within the INSCOM HQs building. 1st IO Cmd has liaison positions established at the Pentagon, NSA, JFCC-NW, CAC, USAIOP/EWP, Joint Information Operations Warfare Command/Air Force IO Command, US Army Special Operations Command at Fort Bragg, USCENTCOM, and the National Air and Space Intelligence Center. 1st IO Cmd has Regional Computer Emergency Response Teams (RCERT) at Fort Gordon, Fort Huachuca, Mannheim Germany, Camp Walker Korea, Fort Shafter and Camp Arifan Kuwait.

https://www.1stiocmd.army.mil/io_portal/Public/Pages/Public_Main.cfm (Requires current CAC card for access.)

Last Updated: September 2007

Army - Army Reserve Information Operations Command (ARIOC)



Mission: The Army Reserve Information Operations Command provides Full-Spectrum Information Operations planning capabilities to support Joint Force and Army missions.

Tasks:

- **Command and Control Army Reserve Information Operations forces**
- **Provide full-spectrum IO planning to support Army Corps, Joint Force Land Component Commander, and Combatant Commanders.**
- **Conduct Information Assurance Operations.**
- **Conduct Computer Network Operations.**
- **Establish Reach Forward capability.**
- **Deploy forward elements to supported Theater.**
- **Assist in Developing IO doctrine.**
- **Computer Emergency Response Teams (CERT)**
 - Deploy RCERT SWA team to Kuwait
 - Support to 1st IO Command and Army Regional CERTs
 - Monitoring Defense Research and Engineering Network (DREN)
 - Provide IO Team Support to JFCC-NW
- **Information Operations Field Support Teams (FST)**
 - Deploy FSTs in Iraq and Afghanistan
 - Employ combat skills of experienced, senior grade staff and contribute to the GWOT
- **Vulnerability Assessment Teams (VAT)**
 - USAR Regional Readiness Command vulnerability assessment
 - Support for Defense Information Technology Security Certification and Accreditation Program (DITSCAP)
 - Support 1st IO Cmd VAT missions
 - Support Army Net Risk Assessment Mission
- **ARIOC Network**
 - Run a secure, stand-alone unclassified network for collaboration, testing, analysis, doctrine development, and ARIOC-wide exercises
 - Provide operational capabilities using geographically separated teams
 - Participate in Joint level exercises with JFCOM Joint IO Range

Subordination: The ARIOC is a subordinate unit of the U.S. Army Reserve Readiness Command, Fort Jackson, SC. ARIOC receives operational tasking through the Army G-3 (Director of Operations, Readiness and Mobilization) and Forces Command (FORSCOM).

Leadership: The Commander of the ARIOC is an Army Reserve Colonel (O-6).

Location: ARIOC HQ is in Adelphi, MD at the Army Research Lab, Phone: 301.394.1190 or DSN 290-1190, S3 - 301.394.1144 or DSN 290-1144.

Last Updated: December 2007

United States Army Information Operations Proponent (USAIOP)



The U.S. Army Information Operations Proponent (USAIOP) is **charged with institutionalizing Information Operations (IO) solutions across Army Doctrine, Operations, Training, Manpower, Logistics, Personnel, and Facilities (DOTMLPF) in order to establish IO as a core Army competency.**

As the Army Proponent for Information Operations (IO), the Commanding General, US Army Combined Arms Center (CG, CAC) established the USAIOP as a CAC major subordinate organization in December 2005 to serve as his executive agent for accomplishing this critical mission. The major responsibilities of USAIOP are derived from CG, CAC's intent for IO, which includes, among other things, the desired end state and eight essential tasks.

a. End State: IO capabilities, capacity, expertise, and Army culture which help achieve an operational advantage that contributes to mission accomplishment.

b. Key Tasks:

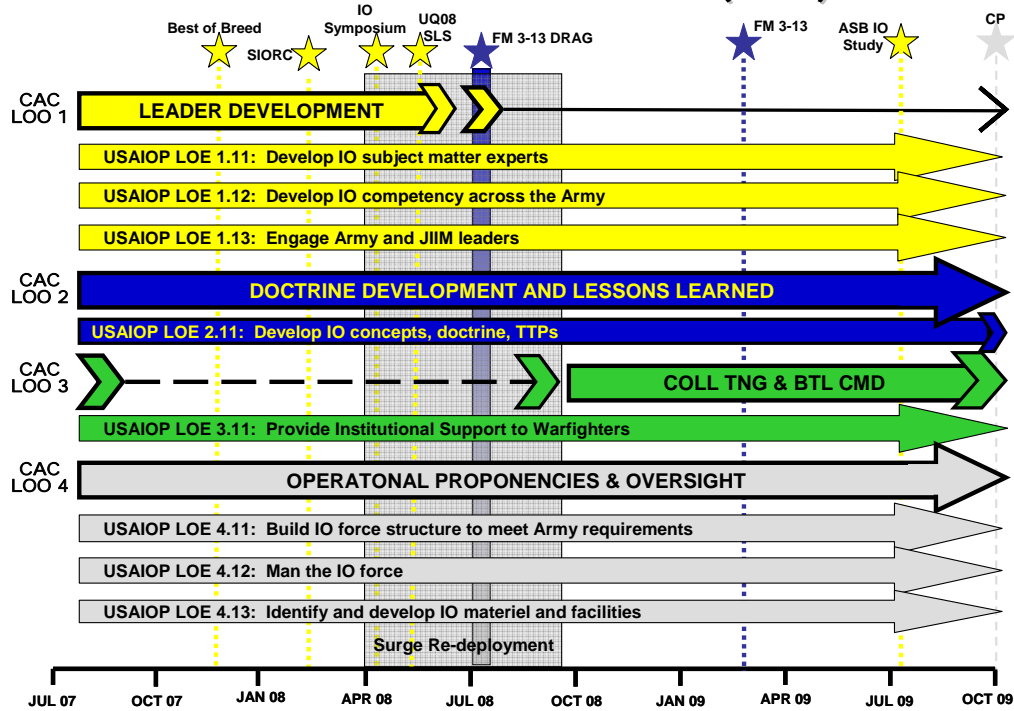
- (1) IO Concepts, Doctrine, and TTPs
- (2) Institutional Support to Warfighters
- (3) IO Subject Matter Experts
- (4) IO Competency Across the Army
- (5) IO Force Structure
- (6) FA30 Personnel Life Cycle
- (7) IO Materiel and Facilities
- (8) Key Leader Engagement

c. The eight key tasks are nested with CG, CAC's four overarching tasks for CAC:

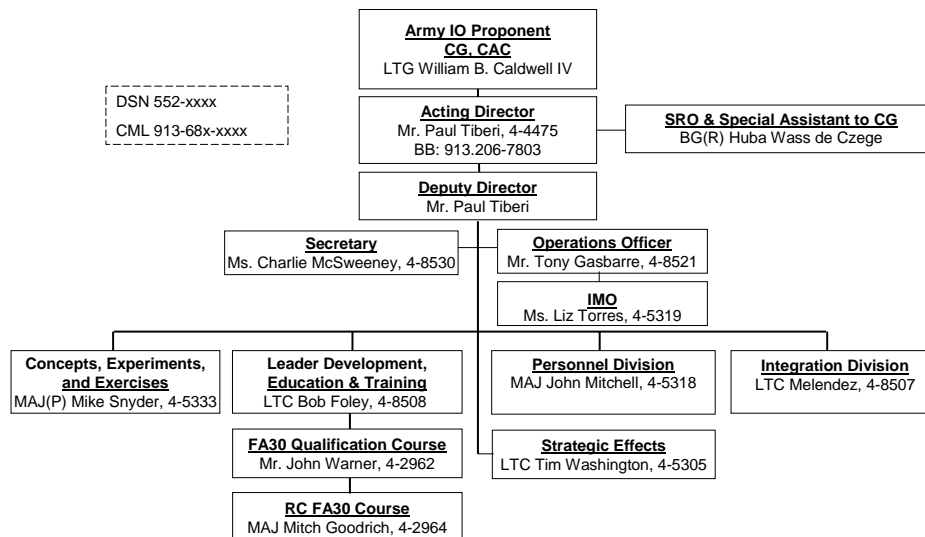
- (1) Leader Development
- (2) Doctrine Development and Lessons Learned
- (3) Collective Training and Battle Command
- (4) Operational Proponencies and Oversight

d. Each of the eight IO tasks translates into a line of effort that is nested with CG, CAC's lines of operation:

USAIOP Lines of Effort (LOE)



e. USAIOP is organized as follows to accomplish this mission:



f. Public Website: <http://usacac.army.mil/CAC/usaiop.asp>

Last Updated: October 2007

Navy - U.S. Navy Information Operations Organizations



This section presents brief descriptions of selected U.S. Navy Information Operations organizations.

- **Naval Network Warfare Command**

Naval Network Warfare Command (NAVNETWARCOM) provides the Navy's central operational authority and type commander for IO in support of naval forces afloat and ashore. NAVNETWARCOM maintains responsibility for identifying, coordinating, and assessing the Navy's IO requirements and FORCEnet architecture development. As the functional component for IO under U.S. Strategic Command, NAVNETWARCOM is responsible for the Navy's strategic IO planning and operational support.

- **Navy Information Operations Command Norfolk**

Navy Information Operations Command (NIOC) Norfolk, the Navy's Center of Excellence for IO, is responsible for providing operationally focused training; planning support and augmentation from the tactical to the strategic level; developing IO doctrine, tactics, techniques, and procedures; advocating requirements in support of future effects-based warfare; conducting experimentation for evaluating emerging or existing IO technologies and doctrine; providing and managing IO data for fleet operations. NIOC Norfolk operates under the operational and administrative control of NAVNETWARCOM, and has two subordinate commands: NIOC San Diego and NIOC Whidbey Island.

- **Navy Cyber Defense Operations Command**

The Navy Cyber Defense Operations Command (NCDOC) (formerly NAVCIRT), coordinates, monitors, and oversees the defense of Navy computer networks and systems, including telecommunications, and is responsible for accomplishing computer network defense (CND) missions as assigned by NAVNETWARCOM and Joint Task Force - Global Network Operations (JTF-GNO).

- **Navy Information Operations Command Suitland**

Navy Information Operations Command (NIOC) Suitland serves as Navy's IO innovation center and functions as the principal technical agent for research and development of prototype IO capabilities. NIOC Suitland supports the development capabilities encompassing all aspects of IO attack, protect, and exploit; maintaining an aggressive program to acquire and analyze state-of-the-art technologies (software and hardware), evaluate fleet applicability, and prototype developmental capabilities. NIOC Suitland maintains a collaborative relationship with Space and Naval Warfare Systems Command, Systems Center San Diego to provide efficient and effective technical expertise in command, control, communications, computers, intelligence, surveillance, reconnaissance and information operations.

NIOC Suitland also supports development coordination between NAVNETWARCOM, OPNAV, NIOC Norfolk, systems commands, IO technology center, and the commercial industry.

Last Updated: October 2007.

Air Force Intelligence, Surveillance and Reconnaissance Agency



Air Force Intelligence, Surveillance and Reconnaissance Agency, with headquarters at Lackland Air Force Base, Texas, was activated June 8, 2007. Formerly known as Air Intelligence Agency, the new Air Force Intelligence, Surveillance and Reconnaissance Agency is aligned under the Air Force Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (A2) as a Field Operating Agency.

Mission

The agency's mission is to organize, train, equip, and present assigned forces and capabilities to conduct intelligence, surveillance and reconnaissance for combatant commanders and the nation. Implement and oversee execution of HQ USAF/A2 policy and guidance to expand Air Force ISR capabilities to meet current and future challenges

Personnel: The agency's 12,000 people serve at approximately 72 locations worldwide.

Organization

The 70th Intelligence Wing, National Air and Space Intelligence Center and Air Force Technical Applications Center are aligned under Air Force ISR Agency. The agency is also responsible for mission management and support of signals intelligence operations for the 67th Network Warfare Wing, Air Force Information Operations Center, 55th Wing and the 480th Intelligence Wing, all four of which are subordinate to Eighth Air Force. Mission support includes organizing, training and equipping the cryptologic elements of these organizations.

70th Intelligence Wing

The 70th Intelligence Wing, with headquarters at Fort Meade, Md., integrates Air Force capabilities into global cryptologic operations, directly supporting national-level decision makers, combatant commanders and tactical warfighters. The wing works closely with the National Security Agency, leveraging the net-centric capabilities of a worldwide signals intelligence enterprise to conduct National-Tactical Integration for the joint and Air Force fight. The effect on the battlespace is immediate, high-impact and decisive. The wing includes six operational intelligence groups located in the continental U.S., Pacific and European theaters. The wing was activated on Aug. 16, 2000.

National Air and Space Intelligence Center (NASIC)

The National Air and Space Intelligence Center, with headquarters at Wright-Patterson AFB, Ohio, is the primary Department of Defense producer of foreign air and space intelligence. NASIC develops its products by analyzing all available data on foreign aerospace forces and weapons systems to determine performance characteristics, capabilities, vulnerabilities, and intentions. NASIC assessments are often an important factor in shaping national security and defense policies. As the DoD experts on foreign aerospace system capabilities, the center also supports weapons treaty negotiations and verification. Since 1961 the center's mission and resources have expanded to meet the challenge of worldwide technological developments and the accompanying national need for aerospace intelligence. In recent years, the

emphasis has increasingly shifted toward evaluation of worldwide aerospace systems and the production of tailored, customer-specific products.

Air Force Technical Applications Center (AFTAC)

The Air Force Technical Applications Center, with headquarters at Patrick AFB, Fla., performs nuclear treaty monitoring and nuclear event detection. AFTAC provides national authorities quality technical measurements to monitor nuclear treaty compliance and develops advanced proliferation monitoring technologies to preserve our nation's security. AFTAC has been performing its nuclear event detection mission since its inception in 1973.

Air Force Information Operations Center (AFIOC)

AF ISR Agency provides mission management and support for specific intelligence operations within the Air Force Information Operations Center. With headquarters at Lackland AFB, Texas, AFIOC is engaged in myriad activities as the Air Force's information operations executive agent, including integrating information operations tactics, training and technology for combatant commanders. The center is comprised of approximately 1,000 military and civilian members trained in the areas of operations, engineering, operations research, intelligence, radar technology and communications and computer applications. AFIOC's lineage dates to 10 Sep 1993, when the Air Force Information Warfare Center was established from elements of the Air Force Cryptologic Support Center and Air Force Intelligence Command. The organization was renamed the Air Force Information Operations Center on 1 Oct 2006 to better reflect its mission and support to combatant commanders.

67th Network Warfare Wing

AF ISR Agency provides mission management and support for specific intelligence operations within the 67th Network Warfare Wing. With headquarters also at Lackland AFB, the 67th NWW has a global mission. As the USAF's cyberspace force and newest combat wing, the 67th NWW's mission is to organize, train, and equip cyberspace forces to conduct network defense, attack, and exploitation.

55th Wing

AF ISR Agency provides mission management and support for specific intelligence operations within the 55th Wing. With headquarters at Offutt AFB, Neb., the 55th conducts worldwide reconnaissance; command, control and communications; Presidential support and international treaty verification as directed by the President, Secretary of Defense, Joint Chiefs of Staff, theater combatant commanders, commanders of major Air Force commands and national intelligence agencies.

480th Intelligence Wing

AF ISR Agency provides mission management and support for specific intelligence operations within the 480th Intelligence Wing. With headquarters at Langley AFB, Va., the 480th produces and provides timely, tailored intelligence data and capabilities to meet Air Force needs. As a dynamic, worldwide force multiplier, it delivers valuable information to U.S. combatants across the globe. The wing performs imagery intelligence, cryptologic and measurement and signatures intelligence activities, targeting and general intelligence production, intelligence data handling system network operations, and data/product dissemination. Subordinate to the wing are three intelligence groups located in the continental U.S. The wing was activated Dec. 1, 2003.

Point of Contact

Air Force ISR Agency, Public Affairs Office; 102 Hall Blvd, Ste 234; San Antonio, TX 78243-7089; DSN 969-2168 or (210) 977-2168.

Web site: <http://www.afisr.af.mil/>

Last updated: June 2007

Air Force Information Operations Center (AFIOC)



AFIOC is located at Lackland Air Force Base, San Antonio, Texas. Collocated with the 67th Network Warfare Wing and Air Force Intelligence, Surveillance, Reconnaissance Agency (AFISRA) formally known as the Air Intelligence agency (AIA). AFIOC is the Air Force Information Operations Center of excellence dedicated to deliver proven Information Operations capabilities integrated across air, space and cyberspace domains. AFIOC originally activated as the 6901st Special Communication Center in July 1953, and became the Air Force Electronic Warfare Center in 1975. Air Force successes in exploiting enemy information systems during Operation Desert Storm led to the realization that the strategies and tactics of command and control warfare could be expanded to the entire information spectrum and be implemented as information warfare. In response, the Air Force Information Warfare Center (AFIWC) was activated on September 10, 1993, combining technical skill sets from the former AFEWC with the Air Force Cryptologic Support Center's Securities Directorate and intelligence capabilities from the former Air Force Intelligence Command. In 2000, AFIWC reorganized to align more closely with the other warfare centers with the formation of the 318th Information Operations Group, which was given the responsibility of operationalizing IW. Soon after, Air Force doctrine for Information Warfare began the transition to Information Operations. On 1 October 2006, AFIWC, was re-designated the Air Force Information Operations Center (AFIOC). The name was changed to better reflect the center's continued advancements in network warfare, electronic warfare and influence operations missions while leading ACC, Air Force and Department of Defense, in information operations integration into combat power. On 1 May 2007, AFIOC was realigned under the Eighth Air Force as part of the Air Force Provisional Cyber Command at Barksdale AFB, LA. The AF Provisional Cyber MAJCOM will work to meet the Chief of Staff's Intent of

- Redefine airpower to extend global reach and power into cyberspace
- Integrate the Air Forces global kinetic and non-kinetic strike capability through the full range of military operations
- Provide combat ready cyber forces to integrate with air and space operations
- Develop an "on ramp" to transition portions of Eighth Air Force into a MAJCOM Component responsible for the full spectrum of integrated global effects.

The AFIOC team of more than 800 military and civilian members is skilled in the areas of operations, engineering, operations research, intelligence, radar technology, communications and computer applications. The members provide information operations capabilities to the warfighters in U.S. Air Force major commands.

AFIOC MISSION STATEMENT: Deliver proven Information Operations capabilities integrated across air, space and cyberspace domains.

AFIOC MISSION TASKS:

Conduct Technology Exploration and Innovation: Conducts plans and development of Air Force IO programs to satisfy warfighter requirements. AFIOC delivers information operations capabilities to systems such as the Automated Security Incident Measurement System (ASIMS) and the Common Intrusion Detection Director System (CIDDS). The center provides quantitative analysis through modeling and simulation of information warfare activities in Air Force operations. These tailored

analytical products are developed in three primary areas: information warfare modeling and simulation, studies of operational systems and support to information warfare acquisition programs. These systems and programs quickly turn around concepts that provide information operations across domain solutions to Air Force units.

Support Development of AF Cyber Influence Operations Capabilities: Supports the development of advancing cyber applications to human focused warfighting capabilities. AFIOC works through 8th Air Force to redefine the Influence Operations Roadmap for the Air Force and the integration of this capability into warfighting capabilities.

Conduct Vulnerability Assessments and Risk Mitigation: The Air Forces lead unit for executing cyberspace vulnerability assessments for critical AF and DoD systems, enabling information superiority in the face of adversary efforts to exploit and disrupt these systems. AFIOC performs a variety of assessments to include: Information Assurance (IA) System Vulnerability Assessments, Network Integrity Assessments (NIA), and Technology Assessments. AFIOC emulates hostile IO activities to assess protective measures and evaluate defensive responses in AF and joint exercises. AFIOC is the only Air Force unit that provides electromagnetic security assessments for aircraft ensuring proper security measures are taken to protect information transmission and identify areas of interference.

Enhance Electronic Warfare Combat Capabilities: Develops, maintains, and deploys electronic warfare capabilities to Air Force, Army, Navy, DoD customers as well as to coalition partners, in direct support of acquisition, testing, campaign planning, and operations. AFIOC provides responsive, realistic training simulations and conducts EW capability and vulnerability analyses. The center provides threat change analysis, parametric data and is a major contributor to the DoD Electronic Warfare Reprogramming process.

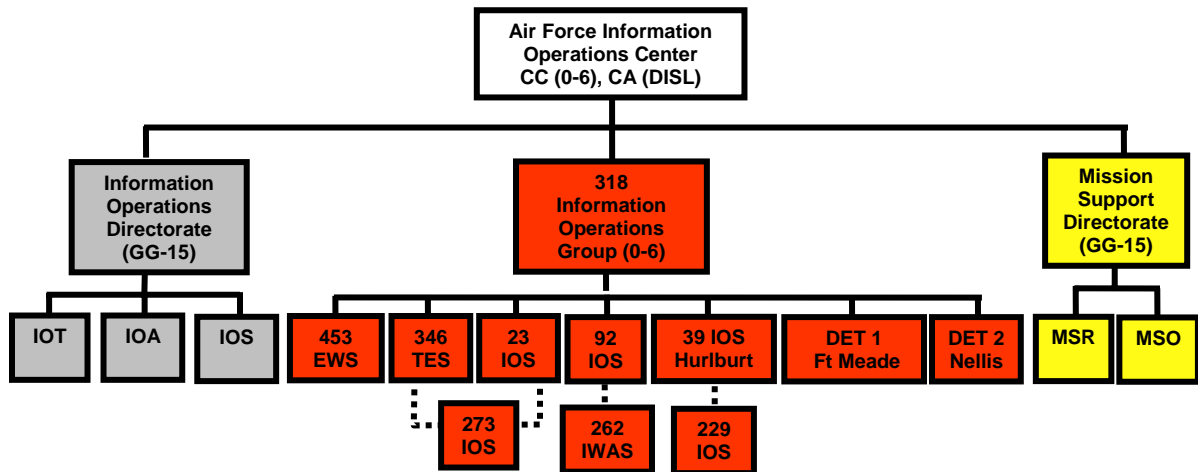
Conduct Information Operations Training, Exercise Support and Tactics Development: Provides training and exercise support to Air Force information operations warriors by integrating network, electronic warfare and influence operations into Air Force and Joint level exercises. AFIOC offers courses such as the Information Operations Integration Course to instruct Air Force members on how to integrate information operations as part of traditional air, space and cyber space employment, thus enhancing combat power. AFIOC is also the focal point for Air Force military deception and counter-deception training and is the executive agent for Air Force operations security training. In 2007 AFIOC developed and executed an Undergraduate Network Warfare Training Course (UNWT) to provide the foundation for Network Warfare Operators.

Integrate with Key Partners: Works closely with key partners to include the Air Force Research Laboratory (AFRL), National Security Agency (NSA), Coalition Forces, and the USAF Weapons School personnel.

Conduct Network Warfare Operations Test and Evaluation: AFIOC is the principal IO test unit in the Air Force that provides test, evaluation and assessment of operational and emerging IO capabilities for operational forces, national agencies, the acquisition community and DoD customers. AFIOC maintains the ACC operational ranges for IO test and training exercises and integrates with the DoD test community in IO testing and training.

Provide Operational Support: Provides operational support to the warfighters to include the 67 Network Warfare Wing, Air Force Office of Special Investigations (AFOSI), and 24/7 Special Communications units. In addition, AFIOC is responsible for updating the IO Joint Munitions Effectiveness Manuals and the Air Force Information Operations Tactics Manual 3-1 Volume 36.

ORGANIZATION:



Last Updated: December 2007

This Page Intentionally Blank

Air Force - Eighth Air Force



Mission:

Headquartered at Barksdale Air Force Base, LA, Eighth Air Force provides integrated long-range global strike, network warfare, battle management, surveillance and reconnaissance, intelligence, tactical air control, and expeditionary heavy construction capabilities to theater combatant commanders. The "Mighty Eighth" also conducts computer network operations as the Air Force component to the Joint Task Force - Global Network Operations, maintains an Air and Space Operations Center supporting USSTRATCOM's Global Strike mission, and trains personnel for worldwide deployment.

Organization

Eighth Air Force was reorganized into a general purpose Numbered Air Force under Air Combat Command with a warfighting mission to support the U.S. Joint Forces and U.S. Strategic Commands in 1992. Eighth Air Force controls assets throughout the United States and at overseas locations worldwide.

In 2001, Headquarters Air Intelligence Agency realigned under ACC as a primary subordinate unit. The agency's two wings realigned under Eighth Air Force. The movement of the 67th Information Operations Wing (Lackland AFB, TX) brought information operations capabilities into a structure similar to those of other Air Force weapons systems provided to commanders.

The Eighth received four additional operational wings as the Air Force moved into the second step of integrating Information Operations into its combat forces in 2002. Eighth Air Force assigned units provide bomber forces, tactical air, electronic warfare, manned and unmanned aerial reconnaissance, intelligence, airborne battle management and command and control, and other capabilities.

The Air Force Network Operations and Security Center (AFNOSC) began operations under Eighth Air Force in 2004 and provided around-the-clock centralized command and control of U.S. Air Force-wide networks. In 2006, the Air Force stood up the Air Force Network Operations Command under Eighth Air Force, re-designating the AFNOSC as the Air Force Network Operations Center (AFNOC), consolidated 10 major command NOSCs into two Integrated NOSCs, and re-designated the 67th as a Network Warfare Wing, to streamline command and control and standardize Air Force network operations in a structure similar to other Air Force weapons systems.. The AFNOC enables the Air Force to maintain its information superiority by providing a single organization to execute both service-specific and joint component responsibilities.

67th Network Warfare Wing: Headquartered at Lackland Air Force Base and subordinate to Air Combat Command's Eighth Air Force, provides network operations and network warfare capabilities to Air Force, joint task force, and combatant commanders. The Wing is charged with operating, protecting, and defending AF networks. In addition to network operations and defense, the Wing provides offensive capabilities of exploitation and attack, as well as communications monitoring. The unique authorities vested in the 67 NWW Commander enable the 67 NWW to provide cryptologic and mission support to

AIA and the AFNetOps Command. The Wing has three subordinate groups: the 26th Network Operations Group (NOG), the 67th Network Warfare Group (NWG), and the 690th Network Support Group (NSG), all collocated at Lackland Air Force Base. The Wing was activated on 1 October 1993 and transitioned to the 67 NWW on 5 July 2006.

Air Force Information Operations Center (AFIOC): In May 2007 Air Force Information Operations Center (AFIOC) located at Lackland Air Force Base (AFB) in San Antonio, Texas was realigned and began operations under Eighth Air Force. AFIOC's team of more than 1,000 military and civilian members are skilled in the areas of operations, engineering, operations research, intelligence, radar technology, communications and computer applications. The members provide improved C2W and information operations (IO) capabilities to the war fighting USAF major commands. AFIOC is responsible for creating the information operations advantage for combatant forces through exploring, developing, applying and transitioning counter information technology, strategy, tactics and data to control the information battle space and providing the world's best IO leaders. AFIOC contributes the DoD's Modernized Integrated Database and the Command and Control Warfare Operational Support Database that provide combat forces with crucial information on adversary military command, control, and communications. AFIOC conducts integrated analysis studies on designated adversaries providing planners with military options beyond the traditional methods of warfare.

Air Force Cyber Command: The mission of newly created AFCYBER will be to integrate the Air Force's global kinetic and non-kinetic capabilities to deliver effects in support of the combatant commander. Given the importance of cyber to modern war fighting operations across all domains, control of the cyber domain has become critical to military operations. The mission of cyber command is to ensure that our forces operating throughout the world can use cyberspace to integrate operations and deliver effects in support of the combatant commander. Ensuring use of the domain will require offensive and defensive operations that not only protect our systems but also deny adversaries the use of their systems as well.

This reorganization takes place as the Air Force continues to blend high-tech information systems with high-tech combat capability. Recent operations demonstrate the need for the fully integrated kinetic and non-kinetic effects-based operations Eighth Air Force continues to pioneer.

Website: <http://www.8af.acc.af.mil/>

Last Updated: September 2007

Information Operations Conditions (INFOCONs)

1. Introduction. The United States Department of Defense Information Operations Condition (INFOCON) system is a commander's alert system that establishes a uniform process for posturing and defending against malicious activity targeted against U.S. DoD information systems and networks. The INFOCON system was developed for U.S. DoD information systems and networks. However, it is acknowledged that U.S. involvement in future conflicts will likely be within a Combined operations environment. This implies that the success of the Warfighting operations will depend greatly on the ability of the U.S. and allied/coalition partners to ensure continued availability and access to critical mission and support information systems and information networks.

2. Description. The INFOCON system is a commander's alert system, characterized by five progressive levels of threats to information networks, and a series of increasing defensive measures that apply to information systems and, to a lesser extent, users of these systems. Specific features assist the commander in using the INFOCON system. A risk mitigation tool aids the commander in proactively declaring postures and directing defensive actions based on advanced indications and warning of hostile activity. The INFOCON system also guides the commander in identifying the INFOCON posture in the event predictive intelligence is not possible. The uniform application of defensive measures promotes predictable responses to crises and provides timely, accurate, and clear direction to commanders. Flexibility is built into the INFOCON system to allow additional specific actions to be mandated, based on the threat. Thus, the INFOCON system provides a range of defensive measures that support operations at all levels of conflict, peacetime operations through combat operations, and back to restoration of peace. The INFOCON system pertains to all information systems and networks, including interconnections between public and coalition networks.

3. Strategy. The INFOCON strategy has shifted from a "threat-based," reactive system to a "readiness-based," proactive approach. This paradigm shift represents a significant change in how commanders at all levels ensure the security and operational readiness of their information networks. While CDRUSSTRATCOM will continue to direct changes in the global INFOCON status, changes in local or regional INFOCON status will now be more actively managed by commanders at all levels (e.g., base, post, camp, station, major command) using a framework of standardized measures. The INFOCONs mirror the Alert System of the Chairman of the Joint Chiefs of Staff, Defense Conditions (CJCS Manual 3402.1B, *ALERT SYSTEM OF THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF (U)*) and are a uniform system of 5 progressive readiness conditions — INFOCON 5, INFOCON 4, INFOCON 3, INFOCON 2, and INFOCON 1. INFOCON 5 is normal readiness and INFOCON 1 is maximum readiness. Each level represents an increasing level of network readiness based on tradeoffs in resource balancing that every commander must make. The INFOCON are supplemented by Tailored Readiness Options (TROs), which are applied in order to respond to specific intrusion characteristics or activities, directed by CDRUSSTRATCOM or commanders.

The INFOCON system is predicated on the fact that a determined intruder will always compromise a networked system. Returning the system to a pristine, baseline state restores confidence in the system. Any system changes, while not always easily detectable in isolation, are almost always detectable by comparing the current status to a previous known baseline. However, maintaining a baseline snapshot across an enterprise and running the appropriate comparisons are non-trivial tasks for network and system administrators. As such, the readiness posture becomes a resource balance of how often commanders want to ensure their networks (or portions thereof) are free of malicious activity in relation to their own Operational Tempo (OPTEMPO). The readiness postures are designed to provide commanders at all levels the flexibility to set the readiness level they deem most appropriate for their OPTEMPO and available resources.

4. Posture Levels.

a. INFOCON 5. INFOCON 5 is characterized by routine NetOps normal readiness of information systems and networks that can be sustained indefinitely. Information networks are fully operational in a known baseline condition with standard information assurance policies in place and enforced.

b. INFOCON 4. INFOCON 4 increases NetOps readiness, in preparation for operations or exercises, with a limited impact to the end user. System and network administrators will establish an operational rhythm to validate the known good image of an information network against the current state and identify unauthorized changes. By increasing the frequency of this validation process, the state of an information network is confirmed as unaltered (i.e., good) or determined to be compromised.

c. INFOCON 3. INFOCON 3 further increases NetOps readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to end-users is minor.

d. INFOCON 2. INFOCON 2 is a readiness condition requiring a further increase in frequency of validation of the information network and its corresponding configuration. The impact on system administrators will increase in comparison to INFOCON 3 and will require an increase in preplanning, personnel training, and the exercising and pre-positioning of system rebuilding utilities. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.

e. INFOCON 1. INFOCON 1 is the highest readiness condition and addresses intrusion techniques that cannot be identified or defeated at lower readiness levels (e.g., kernel root kit). It should be implemented only in those limited cases where INFOCON 2 measures repeatedly indicate anomalous activities that cannot be explained except by the presence of these intrusion techniques. Currently, the most effective method for ensuring the system has not been compromised in this manner is to reload operating system software on key infrastructure servers (e.g., domain controllers, Exchange servers, etc.) from an accurate baseline. The impact on system administrators will be significant and will require an increase in preplanning, personnel training, and the exercising and pre-positioning of system rebuilding utilities. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.

5. Authority. The INFOCON system is established by the Secretary of Defense (SecDef), and administered by the Commander, United States Strategic Command (CDRUSSTRATCOM). The INFOCON system will be administered through the Commander, Joint Task Force - Global Network Operations (JTF-GNO). All combatant commands, services, directors of Defense and combat support agencies will develop supplemental INFOCON procedures as required, specific to their command and in consonance with Strategic Command Directive (SD) 527-1, *DEPARTMENT OF DEFENSE () INFORMATION OPERATIONS CONDITION (INFOCON) SYSTEM PROCEDURES (U/FOUO)*. SD 527-1 can be found on the JTF-GNO SIPRNet webpage:

<http://www.jtfgno.smil.mil/site/index.cfm?Page=INFOCON>

Subordinate and operational unit commanders will use the INFOCON procedures developed by their higher headquarters (e.g., combatant commands or Services). Existing policy and procedures on communications security (COMSEC) may be integrated into local INFOCON procedures at the commander's discretion.

6. Applicability. The established INFOCON procedures (SD 527-1) applies to the Office of the Secretary of Defense, the Services, the Joint Staff, the Combatant Commands, the Defense Agencies, the Field Activities, and all other organizational entities within the (hereafter referred to collectively as "the Components) and any non- Network Operations (NetOps) community of interest (COI) members who are connected to the -wide Global Information Grid (GIG).

7. Assumptions. Several critical assumptions were made about the nature of networks and networking in developing the INFOCON system. Understanding these assumptions is essential to effectively implement this system.

a. Self-imposed Denial of Service. INFOCON measures should not result in a self-imposed denial of service, either to specific users or to entire networks.

b. Operational Synchronization. As military operations continue to rely more and more on net-centric operations, INFOCON measures must be tied directly to the operational activities of the corresponding commands.

c. Implementation Burden. The burden of meeting INFOCON requirements should be placed on network and system administrators rather than on the network's users. This implies that INFOCON measures should, to the extent possible, be transparent to the users.

d. Shared Risk. Due to the interconnectivity of all networks, shared risk is a fact of life. The significance of a clear chain of command within the Components allows for evaluation of the risk associated with any given vulnerability or intrusion. Shared risk is mitigated by the thoughtful and synchronized accomplishment of the systematic measures within a directed readiness level.

e. Insider Threat. Insider threat represents a significant challenge for NetOps and in turn the GIG. The threat is not only from insider personnel but also from outsiders who, because of network trust relationships, are effectively insiders to multiple networks based on compromise of a single network.

f. Incident Response. In most cases, network intrusions detected by analysis or intrusion detection systems are treated as law enforcement events and handled accordingly with respect to conducting the investigation, preserving evidence, and restoring the network. However, under the INFOCON process where a commander desires an increased level of readiness to support on-going or anticipated operations, commanders may decide to forego a law enforcement response to more quickly return the compromised asset to operational status after coordinating with the servicing network defense team.

g. Operational Rhythm. Most information system management activities have a rhythm or cycle of repetition. Increased INFOCON levels may require increased workload and/or decreased cycle time that must be maintained as long as that readiness level is in effect.

h. Information Assurance. The INFOCON measures are not a substitute for operating networks using appropriate IA principles and procedures.

8. Structure. This paragraph explains the INFOCON structure, including level and recommended actions.

a. INFOCON 5, NORMAL READINESS.

INFOCON 5 Procedures

5-1: Re-establish 'secure baseline' in conjunction with a check for unauthorized changes on a semi-annual (180-day) cycle. This should involve mirroring the drives for subsequent examination, prior to re-loading the secure configuration. If examination of the drives indicates unauthorized changes, first determine if the changes were actually authorized, yet improperly recorded. This may reveal the need for a review of the procedures for updating the database of authorized changes. Unauthorized changes may indicate the need to temporarily increase to a higher INFOCON level, depending on what unauthorized changes are discovered. Without a provision such as this, you may be unaware that your network has been compromised.

5-2. Ensure all Information Systems are compliant with guidance and responsibilities outlined within IAW I O-8530.2, *Support to Computer Network Defense* and CJCS Manual 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*.

5-2.1. Update and maintain Anti-Virus, firewall, Information Assurance Vulnerability Alerts (IAVA), and Access Control Lists (ACL) configurations.

5-2.2. Ensure complexity and periodicity of passwords.

5-3. When moving into/from a higher INFOCON level, acknowledge receipt, report entry into INFOCON Level activities via operational channels to the declaring command. Chapter 5 provides sample reporting formats.

5-4. Through automated and procedural means, update and maintain a current database of the following characteristics of all critical network infrastructure equipment used to maintain the network (i.e., routers, firewalls, servers, etc) and a representative sampling of workstations (hereafter called "critical equipment.") Institute appropriate procedures to ensure baseline is continuously updated to reflect authorized modifications.

5-4.1. User Accounts

5-4.2. Groups

5-4.3. Users in Groups

5-4.4. User/Admin/Group Permissions

5-4.5. Executable files (.exe .com .cmd .vbs .vbe .js .jse .wsf .wsh .dll)

5-4.6. Running Services / Open Ports

5-4.7. Registry keys

5-5. Ensure auditing/logging to record, at a minimum: successful and unsuccessful login attempts; file system modifications; and privilege changes. Ensure weekly log review for evidence of abnormal or malicious activity.

5-6. Establish procedures, training, equipment, and administrator certification for the rapid and consistent reestablishment of software baselines for critical equipment.

5-7. Perform operational impact assessment on all mission critical, mission support, and administrative information systems and networks. (Assessing the impact of CNA on our ability to conduct military operations is key to conducting damage assessment, prioritizing response actions, and assisting in identifying possible adversaries. Identify all critical information systems.)

5-8. Conduct routine vulnerability assessments.

b. INFOCON 4, INCREASED MILITARY VIGILANCE.

INFOCON 4 Procedures

- 4-1.** Acknowledge receipt/entry into INFOCON 4 and report again upon completion of the first INFOCON 4 cycle.
- 4-2.** Confirm completion of directive measures at previous INFOCON levels.
- 4-3.** Establish exit criteria. (Declaring Command)
- 4-4.** Implement TROs as specified in the implementing message or by regional/local commanders.
- 4-5.** On a 90 day cycle: Upon notification immediately complete the following activities and then every 90 days thereafter. Using manual methods or available automated tools, identify and verify all changes to the system parameters tracked using the database created at INFOCON 5 (step 5-4.) Investigate all unauthorized changes and remove or terminate as appropriate. If this is being conducted automatically, apply the comparison to all servers and workstations. If manual, apply the comparison to critical equipment and a representative sample of workstations.
- 4-6.** If explicit permissions are used on folders or files also check to ensure permissions have not been modified.
- 4-7.** Verify service accounts that have administrative privileges on critical equipment and ensure that they cannot log on remotely.
- 4-8.** Disable LanMan Hash from all critical equipment if technically feasible.
- 4-9.** Conduct offline rehearsals for the rapid and consistent reestablishment of baselines for SIPRNET and NIPRNET critical equipment as called for in INFOCON 3 Procedures.

c. INFOCON 3, ENHANCED READINESS.

INFOCON 3 Procedures

- 3-1.** Acknowledge receipt and entry into INFOCON 3 and report again upon completion of the first INFOCON 3 cycle
- 3-2.** Confirm completion of directive measures at previous INFOCON levels to the declaring Command.
- 3-3.** Establish exit criteria for current INFOCON level (Declaring Command)
- 3-4.** Implement TROs as specified by implementing message or regional/local commanders.
- 3-5.** Re-establish a secure baseline on a 60-day cycle.
- 3-6.** Conduct offline rehearsals for the rapid and consistent reestablishment of baselines for SIPRNET and NIPRNET critical equipment as called for in INFOCON 2 Procedures.

d. INFOCON 2, GREATER READINESS.

INFOCON 2 Procedures

- 2-1.** Acknowledge receipt and entry into INFOCON 2 and report again upon completion of the first INFOCON 2 cycle.
- 2-2.** Confirm completion of directive measures at previous INFOCON levels to the declaring Command.
- 2-3.** Establish exit criteria for current INFOCON level. (Declaring Command)
- 2-4.** Implement TROs as specified by implementing message or regional/local commanders.
- 2-5.** Re-establish a secure baseline on a 30-day cycle.
- 2-6.** Reestablish known good software baselines on the following servers, PDC/BDC//DNS/Web server. As stated above, this step is intended to address the intrusion techniques that cannot be identified or defeated by other means. These modifications to the servers may be accomplished anywhere within the established operational rhythm period, at the local commander's discretion to reduce impact on operations or resources.
- 2-7.** Conduct offline rehearsals for the rapid and consistent reestablishment of baselines for SIPRNET and NIPRNET critical equipment as called for in INFOCON 1 Procedures.

e. INFOCON 1, MAXIMUM READINESS.

INFOCON 1 Procedures

- 1-1.** Acknowledge receipt and entry into INFOCON 1 and report again upon completion of the first INFOCON 1 cycle.
- 1-2.** Confirm completion of directive measures at previous INFOCON levels to the declaring Command.
- 1-3.** Establish exit criteria for current INFOCON level. (Declaring Command)
- 1-4.** Implement TROs as specified by implementing message or regional/local commanders.
- 1-5.** Re-establish a secure baseline on a 15-day cycle.

9. Procedures.

a. Determining the INFOCON. The foremost determining criteria for changing an INFOCON level is the anticipated operational activity and the degree to which those activities are reliant on networked resources. INFOCON levels should be raised prior to the activity to ensure the network is as ready as possible when the operation or exercise begins. Because system and network administrators implement many of the INFOCON measures over a period of time in a pre-determined operational rhythm, commanders should raise INFOCON levels early enough to ensure completion of at least one cycle before the operational activity begins. Recommendations for possible INFOCON changes should be written into OPLANs and CONPLANs.

(1) Commanders should consider OPSEC when determining INFOCON levels to ensure OPSEC and INFOCON processes are coordinated to protect operations. Regional and local commanders should

consider whether INFOCON changes provide an indicator(s) to an adversary and increase INFOCON levels on a random basis to ensure the establishment of INFOCON levels does not become an indicator of planned activity.

(2) Regional or local commanders who are operating in support of other commands shall consider raising the INFOCON levels of all or key portions of their assets to match the level of the supported commander.

(3) The INFOCON system focuses on readiness but threats to the network should still be a consideration for changing INFOCON levels. Indications and Warning or the detection of new network activity from open sources or network sensors represent threats to network readiness.

b. Declaring INFOCONs. The Commander, Joint Task Force - Global Network Operations (CDR JTF-GNO) will recommend changes in INFOCON to CDRUSSTRATCOM. Prior to this recommendation, JTF-GNO will coordinate with the Components to determine the operational impact of changing the INFOCON level. This operational assessment is a critical element in building CDR JTF-GNO's INFOCON change recommendation to CDRUSSTRATCOM. Upon receiving the recommendation from CDR JTF-GNO, CDRUSSTRATCOM will assess, and if necessary, direct a -level INFOCON change. USSTRATCOM will notify Components of a level INFOCON change via a CNEC and/or a INFOCON Alert message. Regional combatant commanders who independently raise INFOCON levels will notify USSTRATCOM (cc JTF-GNO), other combatant commanders, and the services to provide situational awareness and allow them to consider matching the regional level to better support operations.

c. Response Measures.

(1) Common Directive Measures. Actions common to all Components have been identified for each INFOCON level. The directive measures provide a common readiness posture across information systems and networks.

(2) Order of Implementation. When a non-sequential increase in INFOCONs occurs (e.g. from 5 to 3), the directive measures from the skipped INFOCON level(s) will be accomplished. Once the higher INFOCON level has been achieved the lower (skipped) INFOCON level will complete by default.

(3) Directive Measure Exemptions. Components will normally accomplish all actions for the INFOCON level declared. However, local operational realities may require that a commander delay, or even omit implementation of specific INFOCON directive measures. The commander declaring the INFOCON will be informed by subordinate commands of any deviations and/or exemptions from directive measures or any additional actions directed by CDRUSSTRATCOM in the INFOCON Change Alert Message.

(4) Tailored Readiness Options (TROs). In addition to the directive measures the declaring commander may direct the implementation of TROs to counter a specific threat, by region or globally. TROs are supplemental measures to respond to specific intrusion characteristics directed either by CDRUSSTRATCOM or the responsible regional/local commander. They are narrowly focused and meant to supplement the current INFOCON readiness level either globally, regionally or at bases/camps/posts/ stations. Normally, TROs supplement a lower INFOCON level.

(5) Pre-coordination of Directive Measures. To expedite INFOCON change actions, all supporting combatant commanders, service and/or agency units will establish a Memorandum of Agreement or directive to pre-coordinate INFOCON procedures and directive measures with the unified commander(s) they support. The coordination should include a determination of which actions may be implemented immediately, and which actions require combatant commander notification prior to implementation. This same process applies to all activities under Host/Tenant agreements, as well as

organizations employing cross-domain solutions to connect between different security domains or other trust relationships.

d. Reporting. Technical reporting will be accomplished IAW SD 527-1, Chapter 5, Sample Reporting Templates. INFOCONs assess potential and/or actual impact to operations and must be reported through operational channels. Additional guidance on INFOCON reporting follows.

(1) Reporting Channels. Combatant commands, Services, and agencies will report INFOCON changes and SITREPs to the CDR, USSTRATCOM: USSTRATCOM OFFUTT AFB NE//CC//.

(2) Reporting Frequency. Services, combatant commands, and Defense agencies will report acknowledgement of INFOCON change alert upon receipt of INFOCON Alert Message using the INFOCON Change Acknowledgement SITREP. Services, combatant commands, and Defense agencies will report INFOCON status changes using the INFOCON Status SITREP.

(3) Report Formats. Examples of report formats can be found in SD 527-1, Chapter 5, Sample Reporting Templates.

(4) Dissemination of INFOCON. USSTRATCOM will notify Components of a -level INFOCON change via a CNEC and/or a INFOCON Alert message. Commands, Services, and agencies are responsible for notifying units assigned to them.

10. Security. Classification guidance and disclosure policy concerning IO is addressed in I 3600.2, *Classification Guidance for Information Operations*. Specific guidance related to INFOCON follows.

a. INFOCON labels and descriptions are unclassified.

b. Generic defensive measures, when not tied to a specific INFOCON, are unclassified. Specific measures may be published in a classified appendix, if required.

c. Measures to be taken by all personnel, regardless of INFOCON, are unclassified.

d. General criteria to declare an INFOCON are FOR OFFICIAL USE ONLY (FOUO). Specific criteria may be published in a classified appendix, if required.

e. Classification of the measures associated with a particular INFOCON is the responsibility of the originator and will be classified according to content. However, the measures associated with a particular INFOCON, in aggregate, may require a higher classification than the individual measures. The measures associated with a particular INFOCON, in aggregate, will be FOUO at a minimum.

f. The operational impact of a successful information attack is classified SECRET or higher.

g. CNA intelligence assessments are classified SECRET or higher.

h. Information associated with an ongoing criminal investigation of a CNA may be considered law-enforcement sensitive.

i. A combatant command, Service, or agency may authorize release of its INFOCON system and procedures to allies or coalition partners as necessary to ensure effective protection of its information systems. Locally developed INFOCON procedures should use I 3600.2 and the guidance above when considering release to allies or coalition partners.

j. Changes in INFOCON are operational security (OPSEC) indicators and must be protected accordingly. The criteria and response measures are also of value to foreign intelligence Services in

assessing the effectiveness of a CNA and in analyzing 's response. Do not post INFOCON procedures in publicly accessible locations such as unit web pages on unclassified networks and bulletin boards accessible to outsiders.

11. Relationship of INFOCON to Other Alert Systems. The INFOCON, THREATCON, DEFCON, CNA-WATCHCON, and conventional WATCHCON all interact with each other when the situation warrants it. The INFOCON may be changed based on the world situation (THREATCON, DEFCON), the intelligence community's level of concern (CNA-WATCHCON, conventional WATCHCON), or other factors. Likewise, a change in INFOCON may prompt a corresponding change in other alert systems.

a. The defense condition (DEFCON) is a uniform system of progressive conditions describing the types of actions required to bring a command's readiness to the level required by the situation.

b. The threat condition (THREATCON) is a process that sets the level for a terrorist threat condition at a given location, based on existing intelligence and other information.

c. A watch condition (WATCHCON) is part of the defense warning system indicating the degree of intelligence concern with a particular warning problem.

d. A CNA-WATCHCON is an intelligence assessment that takes into account CNA threat levels, as well as the overall political situation (reference CJCSM 3402.01A, "Alert System of the Chairman of the Joint Chiefs of Staff").

e. The INFOCON addresses risk of attack and protective measures for information and information systems.

Last Updated: October 2007

This Page Intentionally Blank

Glossary

Area of influence	A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. (JP 1-02)
Area of interest	That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. See also area of influence. (JP 1-02)
Civil affairs (CA)	Designated Active and Reserve component forces and units organized, trained, and equipped specifically to conduct civil affairs activities and to support civil-military operations. Also called CA . (JP 1-02)
Civil military operations (CMO)	The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. Also called CMO . (JP 1-02)
Combat Camera (COMCAM)	The acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services. Also called COMCAM. (JP 3-13)
Command and control (C2)	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. (JP1- 02)
Command and control system (C2)	The facilities, equipment, communications, procedures, and personnel essential for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JP 1-02)
Computer network attack (CNA)	Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA . (JP 1-02)
Computer network defense (CND)	Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. Also called CND . See also computer network attack; computer network exploitation; computer network operations . (JP 1-02)
Computer network exploitation (CNE)	Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. (JP 1-02)

Computer network operations (CNO)	Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (JP 1-02)
Computer security (COMPUSEC)	The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02)
Counterdeception	Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (JP 1-02)
Counterintelligence	The information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassination conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)
Counterpropaganda operations	Those psychological operations activities that identify adversary propaganda, contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces. (JP 1-02)
Cyber counterintelligence	Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligences service collection efforts that use traditional methods to gauge cyber capabilities and intentions. (JP1-02)
Cyberspace	The notional environment in which digitized information is communicated over computer networks. (JP 1-02)
Deception action	A collection of related deception events that form a major component of a deception operation. (JP 1-02)
Deception concept	The deception course of action forwarded to the Chairman of the Joint Chiefs of Staff for review as part of the combatant commander's strategic concept. (JP 1-02)
Deception course of action	A deception scheme developed during the estimate process in sufficient detail to permit decision-making. At a minimum, a deception course of action will identify the deception objective, the deception target, the desired perception, the deception story, and tentative deception means. (JP 1-02)
Deception event	A deception means executed at a specific time and location in support of a deception operation. (JP 1-02)
Deception means	Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. physical means Activities and resources used to convey or deny selected information to a foreign power. b. technical means Military materiel resources and their associated operating techniques used to convey or deny selected information to a foreign power. c. administrative means Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 1-02)
Deception objective	The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location. (JP 1-02)
Deception story	A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. (JP 1-02)
Deception target	The adversary decision maker with the authority to make the decision that will achieve the deception objective. (JP 1-02)
Defense support to public diplomacy (DSPD)	Those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government. (JP 1-02)
Desired Effects	The damage or casualties to the enemy or materiel that a commander desires to achieve from a nuclear weapon detonation. Damage effects on materiel are

	classified as light, moderate, or severe. Casualty effects on personnel may be immediate, prompt, or delayed.
Desired perceptions	In military deception, what the deception target must believe for it to make the decision that will achieve the deception objectives. (JP 1-02)
Disinformation	(Army) Disinformation is information disseminated primarily by intelligence organizations or other covert agencies designed to distort information, or deceive or influence US decision makers, US forces, coalition allies, key actors or individuals via indirect or unconventional means. (FM 3-13)
DoDD	Department of Defense Directive.
Electromagnetic pulse (EMP)	The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. (JP 1-02)
Electromagnetic spectrum	The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02)
Electronics security	The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non communications electromagnetic radiation, e.g., radar (JP 1-02)
Electronic warfare (EW)	Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW . The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack . That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA . EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection . That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP . c. electronic warfare support . That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES . Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 1-02)
Global information grid (GIG)	The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 1-02)

Global information infrastructure	The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. (JP 1-02)
High-payoff target	A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through war-gaming, that must be acquired and successfully attacked for the success of the friendly commander's mission. (JP 1-02)
High-value target	A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. (JP 1-02)
Human factors	In Information Operations, the psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals or groups at any level in a state or organization (JP 1-02)
Influence operations	(Air Force) Employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives (AFDD 2-5)
Information	1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)
Information assurance (IA)	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA . (JP1-02)
Information environment	The aggregate of individuals, organizations or systems that collect, process, or disseminate information; also included is the information itself (JP 1-02)
Information management (IM)	The function of managing an organization's information resources by the handling of knowledge acquired by one or many different individuals and organizations in a way that optimizes access by all who have a share in that knowledge or a right to that knowledge. (JP 1-02)
Information operations (IO)	The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own. (D 3600.1/JP 3-13)
Information operations cell	(Army definition, but also functionally described within JP 3-13) A grouping of staff officers to plan, prepare and execute information operations formed around the information operations section. The output of the IO cell is input to the targeting cell. (FM 3-13)

IO capability specialist	A functional expert in one or more of the IO core capabilities (see IO Career Force, below next). They serve primarily in their specialty areas but may also serve as IO planners after receiving IO planner training. (D 3608.11)
IO career force	The military professionals that perform and integrate the core IO capabilities of EW, CNO, PSYOP, MILDEC, and OPSEC. The IO Career Force consists of IO Capability Specialists and IO Planners. (D 3608.11)
IO planner	A functional expert trained and qualified to execute full spectrum IO. They usually serve one or more tours as an IO capability specialist prior to assignment as an IO planner and may hold non-IO positions throughout their careers. (D 3608.11)
INFOCON	Information Operations Condition
Information security (INFOSEC)	The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. (JP 1-02)
Information superiority	The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02)
Information systems (INFOSYS)	The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)
Intelligence	1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.
Interagency coordination	Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged US Government agencies, nongovernmental organizations, and regional and international organizations for the purpose of accomplishing an objective. [JP 1-02]
Joint intelligence preparation of the battlespace (JIPB)	The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the total battlespace environment; describing the battlespace's effects; evaluating the adversary; and determining and describing adversary potential courses of action. The process is used to analyze the air, land, sea, space, electromagnetic, cyberspace, and human dimensions of the environment and to determine an opponent's capabilities to operate in each. Joint intelligence preparation of the battlespace products are used by the joint force and component command staffs in preparing their estimates and are also applied during the analysis and selection of friendly courses of action. (JP 1-02)
Joint restricted frequency list (JRFL)	A time and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. It should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. TABOO frequencies - Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces. Normally, these frequencies include international distress, CEASE BUZZER, safety, and controller frequencies. These frequencies are generally long standing. However, they may be time-oriented in that, as the combat or exercise situation changes, the restrictions may be removed. (JP 1-02)

Joint targeting coordination board (JTCB)	A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance and priorities, and refining the joint integrated prioritized target list. The board is normally comprised of representatives from the joint force staff, all components and, if required, component subordinate units. (JP 1-02)
Measure of effectiveness (MOE)	A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.. (JP 1-02)
Military deception (MILDEC)	Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02)
Network-centric warfare	An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. (Network Centric Warfare: CCRP Publication)
Nongovernmental organization (NGO)	A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 1-02)
Operations security (OPSEC)	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 indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)
Perception management	(Army) Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. (FM 3-13)
Physical destruction	(Army) The application of combat power to destroy or neutralize adversary forces and installations. It includes direct and indirect forces from ground, sea, and air forces. Also included are direct actions by special operations forces. (FM 3-13)
Physical security	1. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. 2. (only) In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. See also communications security; security. (JP1-02)
Priority national intelligence objectives	A guide for the coordination of intelligence collection and production in response to requirements relating to the formulation and execution of national security policy. They are compiled annually by the Washington Intelligence Community and flow directly from the intelligence mission as

	set forth by the National Security Council. They are specific enough to provide a basis for planning the allocation of collection and research resources, but not so specific as to constitute in themselves research and collection requirements.(JP 1-02)
Propaganda	Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. See also black propaganda; grey propaganda; white propaganda. (JP 1-02)
Psychological operations (PSYOP)	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP1-02)
Psychological operations assessment team (POAT)	A small, tailored team (approximately 4-12 personnel) that consists of psychological operations planners and product distribution/ dissemination and logistic specialists. The team is deployed to theater at the request of the combatant commander to assess the situation, develop psychological operations objectives, and recommend the appropriate level of support to accomplish the mission. (JP 1-02)
Psychological operations impact indicators	An observable event or a discernible subjectively determined behavioral change that represents an effect of a psychological operations activity on the intended foreign target audience at a particular point in time. It is measured evidence, ascertained during the analytical phase of the psychological operations development process, to evaluate the degree to which the psychological operations objective is achieved. (JP 1-02)
Psychological operations support element (JPSE)	A tailored element that can provide limited psychological operations support. Psychological operations support elements do not contain organic command and control capability; therefore, command relationships must be clearly defined. The size, composition and capability of the psychological operations support element are determined by the requirements of the supported commander. A psychological operations support element is not designed to provide full-spectrum psychological operations capability; reach-back is critical for its mission success. (JP 1-02)
Public affairs (PA)	Those public information, command information, and community relations activities directed toward both the external and internal public with interest in the . (JP 1-02)
Public diplomacy (PD)	Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. (JP 1-02)
Public information	Information of a military nature, the dissemination of which through public news media is not inconsistent with security, and the release of which is considered desirable or non-objectionable to the responsible releasing agency. (JP 1-02)
Reachback	The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02)
Strategic communication	Focused United States Government (USG) efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the

use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power. (JP 1-02)

Target audience (TA)

An individual or group selected for influence. (JP 1-02.)

The Dictionary of Military and Associated Terms is available on line at:
<http://www.dtic.mil/doctrine/jpreferencepubs.htm>

Last updated : November 2007

* [NOTE: Meaconing is defined (per FM 24-33, "Communications Techniques: Electronic Counter-Countermeasures", July 1990) as the transmission or retransmission of actual or simulated navigation signals to confuse navigation. Meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations].