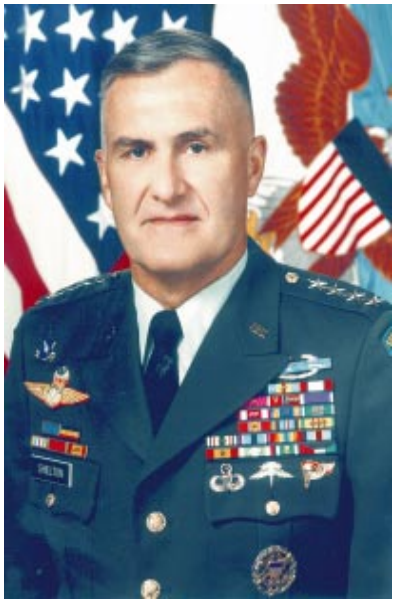
Joint Pub 3-13

Joint Doctrine for Information Operations

9 October 1998



Joint Pub 3-13, "Joint Doctrine for Information Operations," represents a significant milestone in defining how joint forces use information operations (IO) to support our national military strategy. Our ability to conduct peacetime theater engagement, to forestall or prevent crisis and conflict, and to fight and win is critically dependent on effective IO at all levels of war and across the range of military operations.

Joint Pub 3-13 provides the doctrinal foundation for the conduct of IO in joint operations. It discusses integration and synchronization of offensive and defensive IO in the planning and execution of combatant commanders' plans and operations to support the strategic, operational, and tactical levels of war. The guidance contained herein provides joint force commanders and their component commanders with the knowledge needed to plan, train for, and conduct IO.

Commanders must understand the content of this publication and bring it to bear during joint and multinational operations. Please ensure the widest distribution of this and other joint publications, and promote their use at every opportunity.

HENRY H. SHELTON
Chairman
of the Joint Chiefs of Staff

PREFACE

1. Scope

This publication provides the overarching operational guidance for information operations (IO) in the joint context (to include information warfare) throughout the range of military operations. It addresses IO principles relating to both offensive and defensive IO and describes responsibilities for planning, coordinating, integrating, and deconflicting joint IO. Guidance concerning intelligence support to IO, Defense and interagency relationships, and IO in training, exercises, and modeling and simulation also is provided.

2. Purpose

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

3. Application

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

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

Intentionally Blank

TABLE OF CONTENTS

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Defines the Objectives of Information Operations**
- **Addresses the Details of Offensive and Defensive Information Operations**
- **Gives Guidance Concerning Information Operations Planning**
- **Discusses Organizational and Training Issues**

Fundamentals of Information Operations

Employment of information operations (IO) is essential to achieving the objectives of the joint force commander.

Information operations (IO) involve **actions taken to affect adversary information and information systems** while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war. They are a critical factor in the joint force commander's (JFC's) capability to achieve and sustain the level of information superiority required for decisive joint operations.

IO capitalize on the growing sophistication, connectivity, and reliance on information technology. **IO target information** or information systems **in order to affect the information-based process, whether human or automated**. Such information dependent processes range from National Command Authorities-level decision making to the automated control of key commercial infrastructures such as telecommunications and electric power.

Many different capabilities and activities must be integrated to achieve a coherent IO strategy. **Intelligence and communications support** are critical to conducting offensive and defensive IO. The thoughtful **design and correct operation of information systems** are fundamental to the overall conduct of IO. Additionally, to achieve success, **IO must be integrated with other operations** (air, land, sea, space, and special) and contribute to national and military objectives.

Intelligence support is critical to the planning, execution, and assessment of IO. The joint staff intelligence representative(s) assigned to support the IO cell should be the liaison for intelligence support for all IO planning. Intelligence must be timely, accurate, usable, complete, relevant, objective, and sufficiently detailed to support an array of Department of Defense (DOD) IO requirements, including research, development, and acquisition and operational support. **Intelligence preparation of the battlespace is vital to successful IO.** Support from non-DOD and non-US sources also may be required.

Offensive Information Operations

Operations security, military deception, psychological operations, electronic warfare, physical attack/ destruction, special IO, and computer network attack can all provide offensive IO.

Offensive IO involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, **to affect adversary decision makers and achieve or promote specific objectives**. These assigned and supporting capabilities and activities include, but are not limited to, operations security (OPSEC), military deception, psychological operations, electronic warfare (EW), physical attack/destruction, and special information operations (SIO), and may include computer network attack.

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

Defensive Information Operations

The main objective of defensive IO is to help protect and defend information and information systems.

Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO are conducted through information assurance, OPSEC, physical security, counterdeception, counter-propaganda, counterintelligence, EW, and SIO. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. **Offensive IO also can support defensive IO.**

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

Four interrelated processes support defensive IO: information environment protection, attack detection, capability restoration, and attack response. Because they are so interrelated, **full integration of the offensive and defensive components of IO is essential**. JFCs and their subordinate commanders should plan, exercise, and employ available IO capabilities and activities to support integrated defensive IO.

Organization

A fully functional IO cell is paramount to successful IO.

JFCs always should establish a fully functional IO cell. The JFC's staff, which includes the IO cell, develops and promulgates guidance/plans for IO that are passed to the components and supporting organizations and agencies for decentralized planning and execution. The IO cell integrates the broad range of potential IO actions and activities that help contribute to the JFC's desired end state in an area of responsibility or joint operations area. **The organizational structure to plan and coordinate IO should be sufficiently flexible to accommodate a variety of planning and operational circumstances.** IO should be an integral part of all joint military operations. The principal staffs that should be involved in IO planning are the **combatant command**, **subordinate joint force command(s)**, and **component staffs**. It is important to note that the existing command and control warfare cell should be reconfigured to function as the IO cell. This provides the JFC with the capability to integrate, coordinate, and deconflict the full spectrum of IO.

Planning

It is essential for IO planning to be broad-based and to begin at the earliest stages of a joint force commander's campaign or operation planning.

IO planning is accomplished in both the **deliberate and crisis action planning processes** and is **incorporated in the JFC's overall operations planning**. IO planning must be broad-based and encompass employment of all available capabilities — joint, Service, interagency, and multinational. **IO planning must begin at the earliest stage of a JFC's campaign or operation planning.** IO planning must analyze the risk of compromise, reprisal, escalation of hostilities, and uncoordinated or inadvertent counteraction of IO by the various joint, Service, and/or interagency IO capability providers that may be released to the combatant commander for employment.

Training, Exercises, and Modeling and Simulation

Training personnel and organizations responsible for planning and conducting IO on all available capabilities will contribute significantly to successful offensive and defensive IO.

Effective employment of IO in joint operations depends on the **ability to organize and train in the manner the US intends to employ military force**. The basic training task is to train those personnel and organizations responsible for planning and conducting IO. JFCs should ensure that key personnel responsible for planning and conducting IO receive **joint training in both offensive IO and defensive IO**. The Services are responsible for individual and unit training in offensive and defensive IO.

Offensive IO training should include integration of all available and potentially available offensive IO capabilities, to encompass multinational and other DOD and non-DOD offensive capabilities, as well as individual and organizational training. It should also focus on offensive IO training as the main effort and as a supporting function.

Defensive IO training should consist of the integration of all available defensive capabilities, to include commercial and other DOD and non-DOD defensive IO capabilities, and encompassing both individual and organizational training. Defensive IO training should build upon the routine peacetime information and information systems protection and defense procedures used throughout the Department of Defense and other US Government and commercial activities.

CONCLUSION

This publication establishes a detailed understanding of IO. It provides doctrine, principles, and concepts on the fundamentals of IO and its significance in joint operations. The concepts of offensive and defensive IO are extensively addressed, with emphasis on their capabilities and activities. Organization is discussed as a key ingredient to successful IO. Equally important are the strategic, operational, and tactical planning aspects of IO. Finally, the preparation of those personnel and organizations responsible for planning and conducting IO is achieved through extensive training, exercise, and modeling and simulation programs that mirror the manner in which the United States will employ military force.

CHAPTER I
INTRODUCTION

"Generally, in battle, use the normal force [direct approach] to engage; use the extraordinary [indirect approach] to win."

Sun Tzu, The Art of War, tr. Griffith

1. Policy

Department of Defense Directive (DODD) S-3600.1, "Information Operations," and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01A, "Joint Information Operations Policy," outline **general and specific information operations (IO) policy** for Department of Defense (DOD) components and delineate **specific IO responsibilities**. CJCSI 6510.01B, "Defensive Information Operations Implementation," provides specific policy concerning defensive IO.

a. IO involve actions taken to **affect adversary information and information systems while defending one's own information and information systems**. IO apply across all phases of an operation, throughout the range of military operations, and at every level of war. Information warfare (IW) is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries. Within the context of the joint force's mission, the joint force commander (JFC) should apply the term "adversary" broadly to include organizations, groups, or decision makers that may adversely affect the joint force accomplishing its mission. **Defensive IO activities** are conducted on a continuous basis and are an inherent part of force deployment, employment, and redeployment across the range of military operations. **IO may involve complex legal and policy issues** requiring careful review and national-level coordination and approval.

- IO planners must understand the different **legal limitations** that may be placed on IO across the range of military operations.

- IO planners at all levels should consider the following broad areas: (1) **Domestic and international criminal and civil laws** affecting national security, privacy, and information exchange. (2) **International treaties and agreements** and customary international law, as applied to IO. (3) **Structure and relationships** among US intelligence organizations and general interagency relationships, including nongovernmental organizations.

- Geographic combatant commanders should ensure that **IO** are considered in the development of their **theater strategies and campaign plans**.

b. **Contemporary threats** faced by JFCs **are more ambiguous and regionally focused** than during the Cold War. **Combatant commanders may confront a variety of factors that challenge the stability of countries and regions and threaten US national interests and security** within their areas of responsibility (AORs). These instabilities can lead to increased levels of competition, a wide variety of attempts at intimidation, drug trafficking, insurgencies, regional conflicts, and civil war. It is difficult to predict which nations or groups may threaten our interests and how and when such threats will emerge. Even in a time of relative

Launch of DOD satellite

peace, **geographic combatant commanders will be challenged by regional factions seeking to expand their influence by coercion or force**. Some of these potential opponents have **large, modern, conventional military forces equipped with high-quality systems** comparable to those of the Armed Forces of the United States. An adversary's possession of **weapons of mass destruction; ballistic missiles; viable air, land, and naval forces; and sophisticated special operations forces (SOF)** constantly challenge a geographic combatant commander's ability to deter armed conflict and, if necessary, to fight and win. To ensure effective joint operations in such a security environment, **JFCs should have the capability to achieve and sustain information superiority** over their adversaries and potential adversaries. To achieve and sustain information superiority, **JFCs should integrate** the following.

- **Offensive and defensive IO**.
- **Intelligence and other information-related activities** that provide them the timely, accurate, and relevant information on friendly forces, adversaries or potential adversaries, and the battlespace required to achieve their objectives.
- **Activities that leverage friendly information systems**, to include the friendly decision making process.

c. During planning for IO, the **impact** on both friendly and adversary information and information systems must be assessed, especially in regards to the different levels of war. Although IO are conducted at all levels of war, the boundaries between these levels are not distinct. Commanders should be sensitive to the effects IO may have on the levels of war other than that level being planned.

- **IO and the Strategic Level of War.** IO may be included in the spectrum of activities directed by the **National Command Authorities** (NCA) to achieve national objectives by influencing or affecting all elements (political, military, economic, or informational) of an adversary's or potential adversary's national power while protecting similar friendly elements. There may be a high degree of coordination between the military, other US Government (USG) departments and agencies, and allies/coalition partners to achieve these objectives.
- **IO and the Operational Level of War.** IO are conducted to achieve or support campaign or major operation objectives. The focus of IO at this level is on **affecting adversary lines of communication (LOCs), logistics,**

command and control (C2), and related capabilities and activities while protecting similar friendly capabilities and activities. Operational-level IO may contribute to strategic objectives by degrading an adversary's capability to organize, command, deploy, and sustain military forces and capabilities and by allowing the joint force to obtain and maintain the degree of information superiority required to quickly and decisively accomplish its mission.

- **IO and the Tactical Level of War.** IO at this level involve achieving **specific tactical objectives**. The primary focus of these IO is affecting adversary information and information systems relating to C2, intelligence, and other information-based processes directly relating to the conduct of military operations while protecting similar friendly capabilities.

d. Employed as an integrating strategy, **IO focus on the vulnerabilities and opportunities** presented by the increasing dependence of the United States and its adversaries or potential adversaries on information and information systems (See Figure I-1). **Employment of IO is essential to achieving the objectives of the JFC.** In the Department of Defense, the ultimate strategic objective of offensive IO is to **affect adversary or potential adversary decision makers** to the degree that they will cease actions that threaten US national security interests. At the tactical, operational, and strategic levels, IO target and protect information, information transfer links, information gathering and processing nodes, and human decisional interaction with information systems. **IO may have their greatest impact as a deterrent in peace and during the initial stages of crisis.**

e. IO contribute to the **integration of aspects** of the military element of national power with all other elements of national power to achieve objectives. IO can support the overall USG strategic engagement policy throughout the range of military operations. The effectiveness of **deterrence**, **power projection**, and **other strategic concepts** is greatly affected by the ability of the United States to influence the perceptions and decision making of others. In times of crisis, **IO can help deter adversaries from initiating actions** detrimental to the

Figure I-1. Information Operations as a Strategy

interests of the United States or its allies and/or coalition partners. If carefully conceived, coordinated, and executed, **IO can make an important contribution to defusing crises**; reducing periods of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts; and forestalling or eliminating the need to employ forces in a combat situation. Thus IO, at both the national-strategic and theater-strategic levels, **require close coordination among numerous elements of the USG**, to include the Department of Defense. Command, control, communications, and computers (C4) and intelligence provide crucial support to IO (See Figure I-2).

f. **IW can be waged in crisis or conflict** within and beyond the traditional military battlespace. IW may be conducted to shape the battlespace and prepare the way for future operations to accomplish US objectives.

g. Command and control warfare (C2W) is an **application of IO in military operations that specifically attacks and defends the C2 target set**. The capabilities and activities employed in C2W (psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction), as well as other less traditional methods focused on information systems, can be employed to achieve broader IO objectives that are outside the C2 target set.

See JP 3-13.1, "Joint Doctrine for Command and Control Warfare (C2W)," for further C2W guidance.

h. Chairman of the Joint Chiefs of Staff **specific IO policy guidance** is set forth in CJCSI 3210.01A, "Joint Information Operations Policy," as follows.

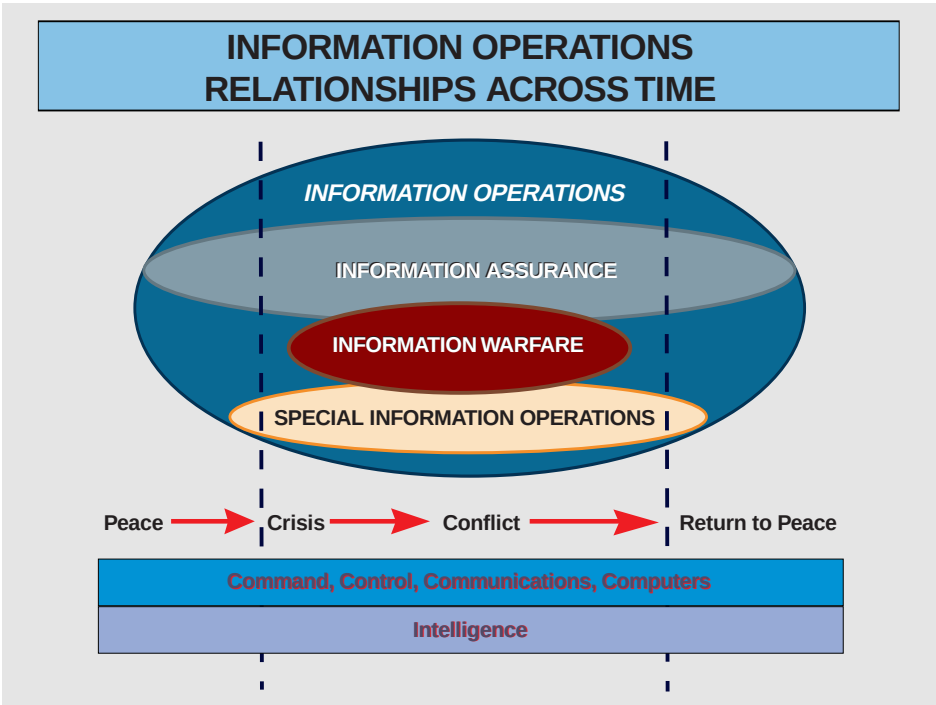


Figure I-2. Information Operations Relationships Across Time

- **Offensive IO** will be employed to achieve mission objectives when deemed appropriate.

- **Information, information systems, and information-based processes** (such as C2, communications, weapons systems) used by US military forces will be protected relative to the value of the information they contain and the risks associated with their compromise or loss of access. The value of information may change in relation to the objectives during peace, crisis, conflict, or postconflict, as well as during the various phases of an operation.

- **Intelligence requirements** in support of IO will be articulated with sufficient specificity and timeliness to the appropriate intelligence production center or other intelligence organizations to meet the IO demand.

See JP 2-01, "Joint Intelligence Support to Military Operations," and JP 2-02, "National Intelligence Support to Joint Operations."

- **Technology** that affects an adversary's information and information systems and protects and defends friendly information and information systems will be pursued at every opportunity to ensure the greatest return on investment.

- **Joint and Service school curricula** will ensure personnel are educated in the concepts of IO, to include an appreciation of the vulnerabilities inherent in their information systems and the opportunities found in adversary systems. Combatant commands and Services will integrate IO into exercises and modeling and simulation (M&S) to enhance overall joint operational readiness.

- **Combatant commanders** will incorporate offensive and defensive IO into deliberate and crisis action planning to accomplish their assigned missions.

"We will have to say that in any cause the decisive role does not belong to technology — behind technology there is always a living person without whom technology is dead."

Mikhail Frunze, quoted in Gareyev, Frunze, Military Theorist, 1985

- The growth in **IO-related technology and capabilities and associated legal**

RC-135 supporting operational commander

issues makes it critical for commanders at all levels of command to involve their staff judge advocates in development of IO policy and conduct of IO.

2. Responsibilities

Listed below are **unclassified responsibilities for key IO individuals and commands or organizations** as shown in DODD S-3600.1, "Information Operations (IO)," CJCSI 3210.01A, "Joint Information Operations Policy," and CJCSI 6510.01B, "Defensive Information Operations Implementation." Additional classified IO responsibilities are located in Appendix A, "Supplemental Information Operations Guidance," (published separately).

a. **Chairman of the Joint Chiefs of Staff**

- Serves as the principal military advisor to the Secretary of Defense on IO matters.
- Validates joint IO requirements, as appropriate.
- Establishes doctrine to facilitate the integration of IO concepts into joint warfare.
- Ensures plans and operations include and are consistent with IO policy, strategy, and doctrine.
- Coordinates with the commanders of combatant commands to ensure effective execution of IO.
- Ensures that exercises and M&S routinely test and refine capabilities, including the application of realistic wartime stress to information systems.
- Ensures joint C2 is sufficiently robust to support continued operations should US information systems be degraded.
- Ensures that IO is a part of joint military education curricula.
- Coordinates with the Director, National Security Agency (NSA), on IO, as appropriate.

b. **Combatant Commanders**

- Plan, exercise, and conduct IO in support of national goals and objectives as directed by the Joint Strategic Capabilities Plan.
- Integrate capabilities into deliberate and crisis action planning to conduct IO in accordance with appropriate policy and doctrine to accomplish their Unified Command Plan-assigned missions.
- Develop a process within the combatant command and subordinate joint force staffs that effectively integrates the various disciplines and capabilities associated with IO.
- Incorporate IO tactics, techniques, and procedures into exercises, M&S, and training events using the Joint Mission Essential Task List process.
- Identify IO requirements and submit appropriate mission needs statements to the Chairman of the Joint Chiefs of Staff for validation.
- Develop and maintain integrated priorities for IO requirements.
- Develop IO intelligence requirements in support of all pertinent operation plans (OPLANs).
- Identify IO M&S requirements to the Joint Warfighting Center.
- Identify IO education and training requirements to the Director for

Operational Plans and Interoperability (J-7).

- Capture IO lessons learned from joint after-action reviews and submit them to the J-7 as part of the joint after-action report.

- Plan and coordinate flexible deterrent options (FDO) using IO capabilities along with traditional FDOs such as shows of force, enforcement of sanctions, maritime intercept operations, military exercises, and M&S.

c. **Chiefs of the Services and Commander in Chief, US Special Operations Command**

- Conduct research, development, testing and evaluation, and procurement of capabilities that meet validated Service and joint IO requirements.

- Maintain liaison with Services, Defense agencies, and other appropriate agencies to minimize duplication of capabilities.

- Identify intelligence requirements necessary to support capabilities being developed or fielded to conduct IO. Coordinate with Defense Intelligence Agency (DIA) and the Joint Staff to ensure these requirements are communicated to the Intelligence Community.

- Incorporate IO into Service school curricula and into appropriate training and education activities. Both offensive and defensive aspects of IO must be addressed.

- Organize forces with capabilities to conduct IO. Train forces to conduct IO. Ensure Services' forces and planning capabilities effectively support the combatant commanders through the appropriate Service component commanders.

- Exercise capabilities to conduct IO across the range of military operations.

- Coordinate with DIA, Defense Information Systems Agency (DISA), and NSA to ensure development and population of data bases supporting collaborative planning, analysis, and execution of IO.

- As required, develop Service IO policy, doctrine, and tactics that both complement emerging joint doctrine and optimize particular Services' capabilities and organization.

d. **Director, National Security Agency**

- Provides information security (INFOSEC) and OPSEC technology, products, and services to help protect against hostile IO efforts.

- Conducts vulnerability and threat analysis to support the defense and protection of US and friendly information and information systems.

- Coordinates with DIA, DISA, and the Services to ensure development and population of data bases supporting collaborative planning, analysis, and execution of IO.

e. **Director, Defense Intelligence Agency**

- Manages Defense Intelligence Community production to support the full range of DOD IO.

- Oversees DOD requirements and serves as the Defense Intelligence Community focal point for the development, management, and maintenance of support data bases and information

systems that facilitate the timely dissemination of all-source, finished intelligence in support of DOD IO.

- As DOD human intelligence (HUMINT) manager, provides oversight, guidance, and direction to the Defense HUMINT Service, consistent with DOD IO.

- Assists combatant commanders with the development of command intelligence architecture planning programs that fully integrate IO support requirements.

- Provides precise and timely intelligence for IO target selection and post-strike analysis to the combatant commands and Joint Staff.

- Provides direct intelligence assistance to the combatant commanders in the planning and execution of IO across the range of military operations.

- Develops standards for Global Command and Control System-compliant IO support data bases and coordinates with the Services, NSA, and DISA to ensure subsequent data base population.

- Provides indications and warning (I&W) of IO attacks, with the assistance of DISA and other government and nongovernment agencies.

- Provides intelligence certification of all weapons acquisition programs for IO in accordance with CJCSI 3170.01, "Requirements Generation System."

f. **Director, Defense Information Systems Agency**

- Ensures measures are taken to employ defensive capabilities to protect the Defense Information Infrastructure (DII).

- Coordinates with DIA, NSA, and the Services to ensure population of data bases supporting collaborative planning, analysis, and execution of IO.

- In coordination with either government and nongovernment agencies, assists DIA in providing I&W of computer network attacks (CNA).

- Maintains liaison with the Office of the Secretary of Defense, the Joint Staff, the combatant commanders, the Services, and Defense agencies to minimize the duplication of effort in defensive IO capabilities development and to ensure interoperability and mutually reinforcing security policies, procedures, and systems.

g. **Director, Joint Command and Control Warfare Center (JC2WC)**

- As requested, provides direct support to joint commanders in accordance with CJCSI 5118.01, "Charter for the Joint Command and Control Warfare Center."

- In concert with the Services, assists in the integration of C2W opposition force (OPFOR) activities conducted in the joint exercise arena.

h. **Commander, Joint Warfighting Center**

- Collects, identifies, and ensures combatant command and Service IO requirements are satisfied by present and future M&S systems.

- Through the M&S Support Activity:

  •• Ensures M&S efforts are coordinated to eliminate duplication of effort and maintain focus on the development of

systems that fulfill combatant command and Service IO training and exercise requirements;

•• Coordinates with the Defense Modeling and Simulation Office to stay apprised of other agency M&S efforts that could support combatant command and Service IO requirements; and

•• Coordinates and assists the Joint Staff, Services, and combatant commanders in developing joint IO doctrine.

i. **All DOD Elements.** Adopt a risk management approach to the protection of their information, information systems, and information-based processes based on potential vulnerability to IO.

3. Terminology

a. The terms listed below and selected other terms used in this publication as well as all abbreviations used are listed in the glossary. **The basic definitions and concepts in this chapter are critical to understanding the rest of this publication.**

b. **"Computer network attack"** is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.

c. **"Information"** is defined as facts, data, or instructions in any medium or form. It is the meaning that a human assigns to data by means of the known conventions used in their representation. The same information may convey different messages to different recipients and thereby provide "mixed signals" to information gatherers and users, to include the intelligence community.

d. **"Information assurance"** is defined as IO that protect and defend 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.

e. **"Information-based processes"** are processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes. Information-based processes may be found in any facet of military operations from combat through combat support and combat service support across the range of military operations, and in other elements of national power. Information-based processes are included in all systems and components thereof that require facts, data, or instructions in any medium or form to perform designated functions or provide anticipated services. For purposes of IO, examples range from strategic reconnaissance systems, to a key adversary decision maker, to a local traffic control point in an austere overseas joint operations area (JOA).

f. The **"information environment"** is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself.

g. **"Information operations"** are actions taken to affect adversary information and information systems, while defending one's own information and information systems. IO require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of C2 with intelligence support. IO are conducted through the integration of many capabilities and related activities. Major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include CNA. IO-related activities include, but are

not limited to, public affairs (PA) and civil affairs (CA) activities (See Figure I-3). There are **two major subdivisions within IO:** offensive IO and defensive IO.

- **Offensive IO** involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives. These assigned and supporting capabilities and activities include, but are not limited to, OPSEC, military deception, PSYOP, EW, physical attack/destruction, and special information operations (SIO), and could include CNA. See Chapter II, "Offensive Information Operations," for further guidance.

- **Defensive IO** integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO are conducted and assisted through information assurance (IA), OPSEC, physical security, counterdeception, counter-propaganda, counterintelligence (CI), EW, and SIO. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Offensive IO also can support defensive IO. This concept is further described in Chapter III, "Defensive Information Operations."

h. **"Information superiority"** is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability

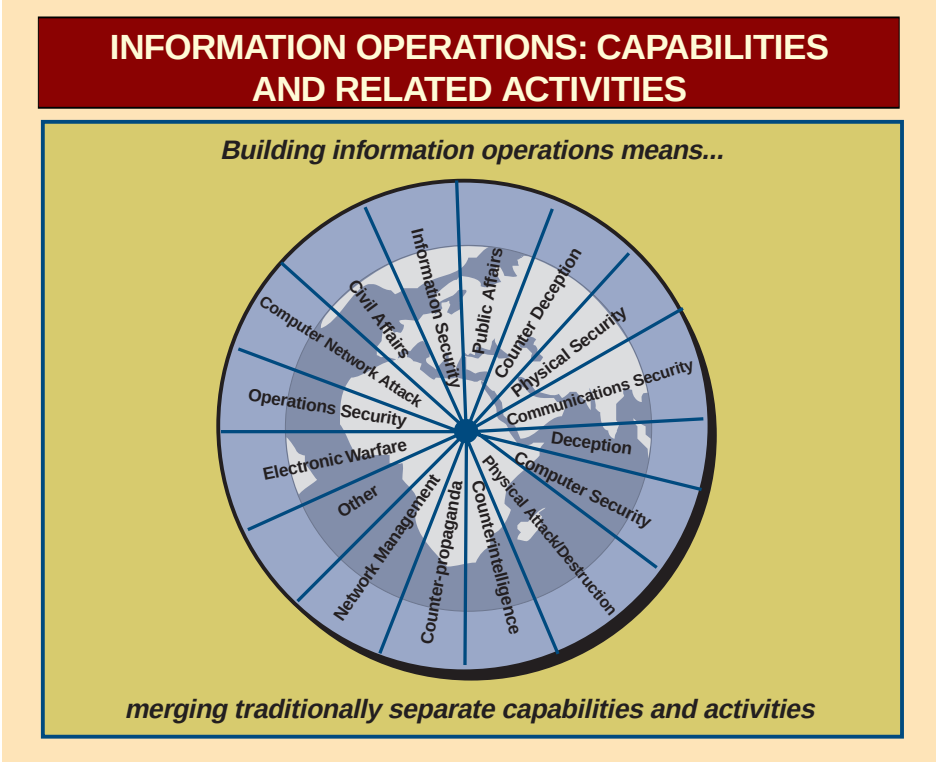


Figure I-3. Informations Operations: Capabilities and Related Activities

to do the same. Information superiority may be all pervasive in the AOR/JOA, or it may be function- or aspect-specific, localized, and temporal.

i. An **"information system"** is the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. The information system also includes the information-based processes.

j. **"Information warfare"** is information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

k. **"Special information operations"** are information operations that, by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the US, require a special review and approval process.

"Force has no place where there is need of skill."

Herodotus,
The Histories of Herodotus

4. Fundamentals of Information Operations

a. **General**

- **Increasingly complex information systems** are being integrated into traditional warfighting disciplines such as mobility; logistics; and command, control, communications, computers, and intelligence (C4I). Many of these systems are designed and employed with **inherent vulnerabilities** that are, in many cases, the unavoidable consequences of enhanced functionality, interoperability, efficiency, and convenience to users. The low cost associated with such technology makes it **efficient and cost effective** to extend the capabilities (and vulnerabilities) to an unprecedented number of users. The **broad access** to, and use of, these information systems enhances warfighting. However, **these useful capabilities induce dependence, and that dependence creates vulnerabilities**. These information systems are a **double-edged sword** — on one edge representing areas that warfighting components must protect, while on the other edge creating new opportunities that can be exploited against adversaries or used to promote common interests (See Figure I-4),

- **IO capitalize on the growing sophistication, connectivity, and reliance on information technology.** IO target information or information systems in order to affect the information-based process, whether human or automated. Such information dependent processes range from **NCA-level decision making** to the **automated control of key commercial infrastructures** such as land- and space-based telecommunications and electric power.

- Many different **capabilities and activities must be integrated** to achieve a coherent IO strategy. **Intelligence and communications support** are critical to conducting offensive and defensive IO. The **thoughtful design and correct operation** of information systems are fundamental to the successful conduct of IO. Moreover, to be successful, **IO must be integrated with other operations** (air, land, sea, space, and special) and contribute to national and military objectives.

- IO support the national military strategy but **require support, coordination, and participation by other USG**

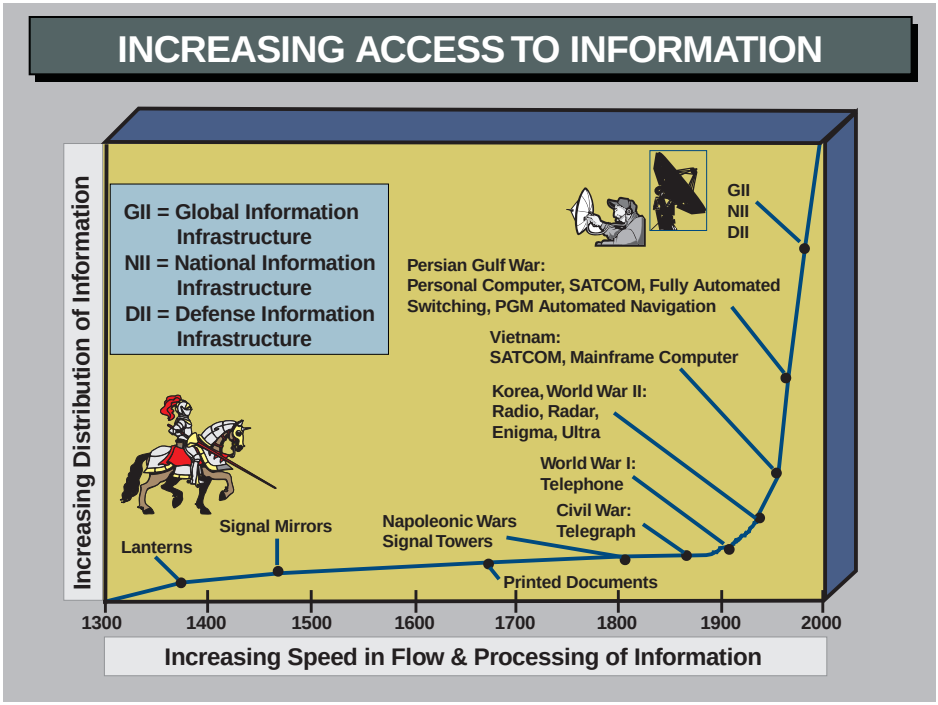


Figure I-4. Increasing Access to Information

departments and agencies as well as commercial industry. Although much of DOD information flows depend on commercial infrastructures, in many cases **the protection of these infrastructures falls outside the authority and responsibility of the Department of Defense**. The Department of Defense assists in demonstrating to service providers the compelling need for a collaborative, teamed approach in crafting solutions — not just to support the Department of Defense and to protect US national security, but to protect their own proprietary interests as well. Offensive and defensive IO actions also require interagency deconfliction and cooperation (See Figure I-5).

- There are several **fundamental legal considerations** that must be taken into account during all aspects of IO planning and execution. The staff judge advocate should be an integral part of the planning and execution of such operations. Legal considerations include, but are not limited to, an assessment of the following.

•• The different legal limitations that may be placed on IO in peacetime, crisis, and conflict (to include war). Legal analysis of intended wartime targets requires traditional Law of War analysis.

•• The legal aspects of transitioning from defensive to concurrent offensive operations.

•• Special protection for international civil aviation, international banking, and cultural or historical property.

•• Actions that are expressly prohibited by international law or convention. Examples include, but are not limited to: (1) Destruction resulting from space-based attack (Convention on

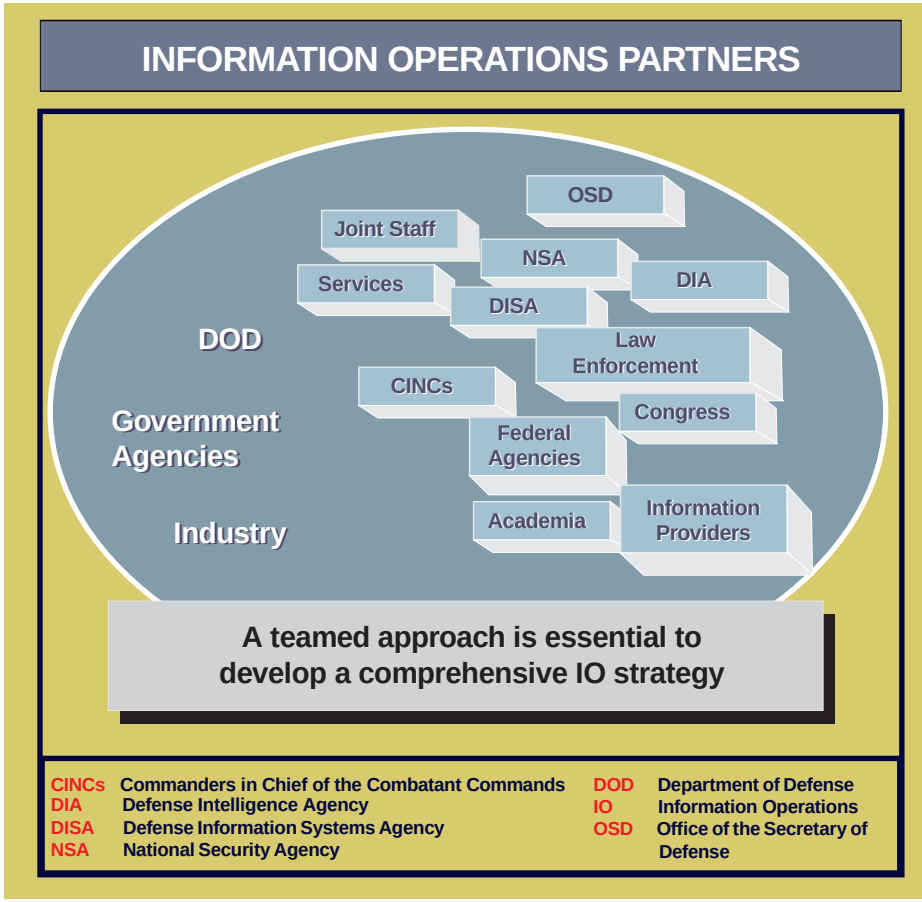


Figure I-5. Information Operations Partners

International Liability for Damage Caused by Space Objects); (2) Violation of a country's neutrality by an attack launched from a neutral nation (Hague Convention V); and (3) PSYOP broadcasts from the sea, which may constitute unauthorized broadcasting (UN Convention on Law of the Sea).

b. **Information Environment.** The growth of information systems and technologies offer **continuing potential for exploiting the power of information in joint warfighting**. The labels placed on information systems and associated networks may be misleading as there are no fixed boundaries in the information environment. **Open and interconnected systems are coalescing into a rapidly expanding global information infrastructure (GII)** that includes the US national information infrastructure (NII) and the DII.

- **The GII is the worldwide interconnection of communications networks, computers, data bases, and consumer electronics** that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites and satellite ground stations, fiber-optic transmission lines, networks of all types, televisions, monitors,

printers, and much more. The GII includes more than just the physical facilities used to store, process, and display information. The personnel who make decisions and handle the transmitted information constitute a critical component of the GII.

- The **NII** is similar in nature and purpose to the GII but relates in scope only to a **national information environment,** which includes all government and civilian information infrastructures.

- **The DII is embedded within and deeply integrated into the NII.** Their seamless relationship makes distinguishing between them difficult. The DII is the **shared or interconnected system** of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The DII **connects DOD mission support, C2, and intelligence computers** through voice, telecommunications, imagery, video, and other multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network. It includes C2, strategic, tactical, intelligence, and commercial communications systems used to transmit DOD information (See Figure I-6).

c. **Reachback Dependencies.** Military planners at all levels of command should understand the **nature**, **complexities**, and **dependencies** of the GII, NII, and DII.

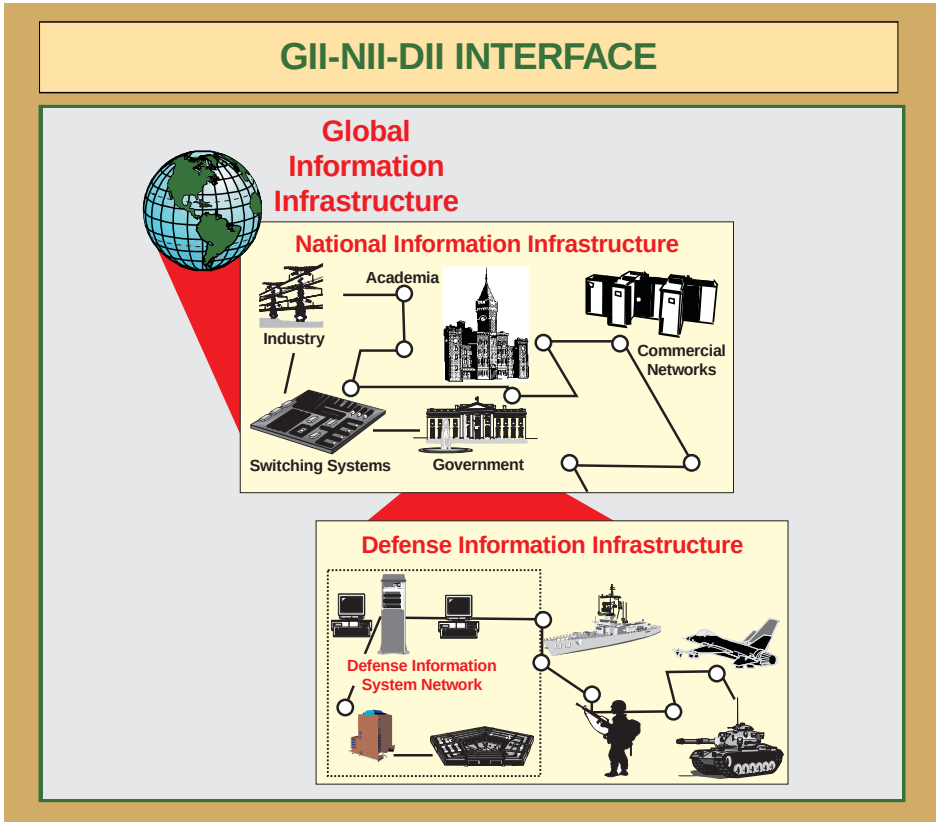


Figure I-6. GII-NII-DII Interface

- The successful conduct of operations requires **access to information available outside the operational area**. Information infrastructures no longer parallel traditional command lines, and warfighters need **frequent, instant, and reliable access to information** at locations in the continental United States as well as in theater. For example, mobility and sustainment of forces are highly dependent on commercial infrastructures that include international telecommunications, the public switched network, commercial satellites and ground stations, transportation systems, and electric power grids. Joint forces require secure video teleconferencing, data base connectivity, direct downlink, and broadcast/receive capabilities for reachback access to intelligence, logistics, and other essential support data. The **technical complexity and management** of these information infrastructures **could inhibit a commander's ability to control the flow of information** or dynamically manage available information and telecommunications resources. To support offensive operations, JFCs may reach back to employ offensive capabilities and techniques to contribute to information superiority, to more effectively achieve objectives, or support other operations in their AOR or JOA.

- Providing capabilities to support crises and contingency operations requires the **expansion of our information infrastructure beyond the established peacetime information environment**. Joint forces must have assurance that this expanded infrastructure can attain the level of protection required to assure mission success. The authority to implement this level of protection for the NII has yet to be assigned to any USG department or agency. Therefore, **the Joint Staff coordinates in the various interagency forums** to demonstrate to service providers the compelling need for a collaborative, teamed approach to ensure friendly forces have access to timely and relevant information wherever and whenever needed.

- **US dependence on information and information systems**, and the resultant vulnerabilities this entails, **exposes the United States to a wide range of threats**. These threats include, but are not limited to, computer hackers, criminals, vandals, terrorists, and nation states, and have brought focus and compelling relevance to our vulnerabilities to emerging technologies. The dramatically increased power and availability of computers and their telecommunications connections and computer applications have set in motion revolutionary capabilities that will enhance and support all aspects of military operations (See Figure I-7).

*"**Information security** takes on added importance in this new age. This will be true whether we find ourselves engaged with a sophisticated foe or involved in a low-intensity conflict. On the other hand, as we look at our opportunities for offensive **information** ops, we will be more limited to situations when we face an opponent who has a similar reliance on **information**. My point is that we run a tremendous risk if we look at **information warfare** only as a unique American advantage. It is not."*

Gen. Ronald R. Fogleman, Air Force Chief of Staff, to the Armed Forces Communications-Electronics Association, Washington, April 25, 1995

d. **IO Target Set.** IO targets are **determined by the JFC's objectives and operations concepts** and are influenced largely by in-depth intelligence analysis. The JFC's IO cell, supported by intelligence,

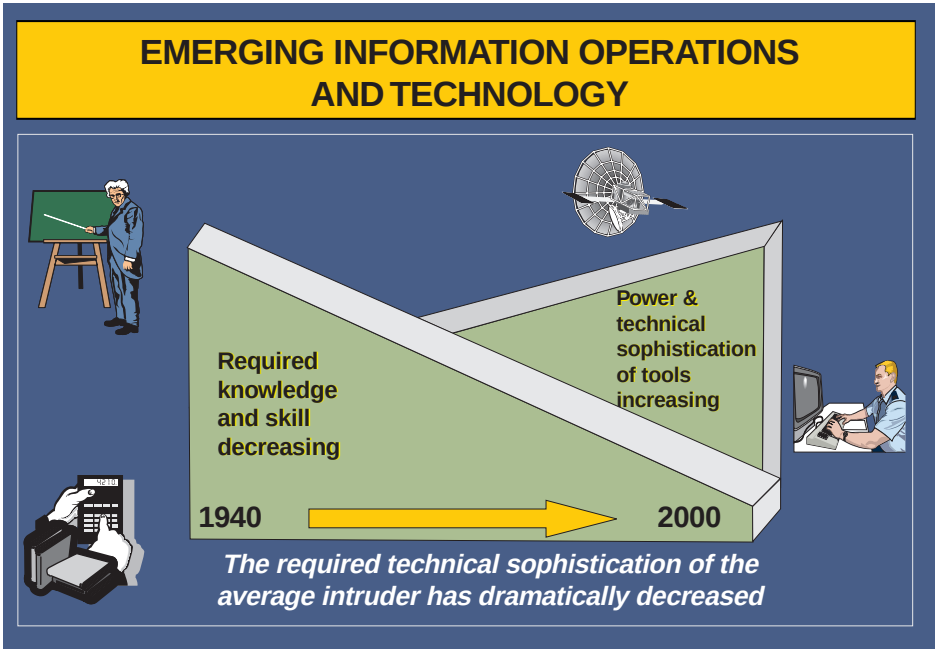


Figure I-7. Emerging Information Operations and Technology

should **analyze data bases and templates** to determine the vulnerabilities and critical elements of friendly and adversary information, information-based processes, and information systems. See Chapter IV, "Information Operations Organization," for additional guidance concerning the IO cell. Examples of potential IO targets are shown in Figure I-8.

- **Early identification of critical elements** with respect to specific IO targets is essential for successful offensive and defensive IO. **Offensive IO may target only a key element** of a specific critical adversary target set and attain great success. Conversely, understanding the nature of the threat will help defend and protect against adversary IO. An IO threat should be defined in terms of a specific adversary's intent, capability, and opportunity to adversely influence the elements of the friendly information environment critical to achieving objectives. An **IO threat** is an adversary that is organized, resourced, and politically sponsored/motivated to affect decision makers. Hackers, criminals and organized crime, insiders, industrial and economic espionage, and, in some cases, terrorism constitute a general threat to the protected information environment. This general threat requires monitoring for indications of a specific IO threat and subsequently may require additional defensive IO measures.

- **C2 remains a substantial target for IO.** Commercial communications systems linked to friendly and adversary C2 systems offer unique challenges to offensive targeting and defensive protection.

- **Examples of key areas of warfare support** comprising potential offensive target sets and requiring protection include, but are not limited to, **logistics**, **intelligence**, and **non-C2 communications systems**. Friendly commercial infrastructures also may be targeted by an adversary's offensive capabilities, just

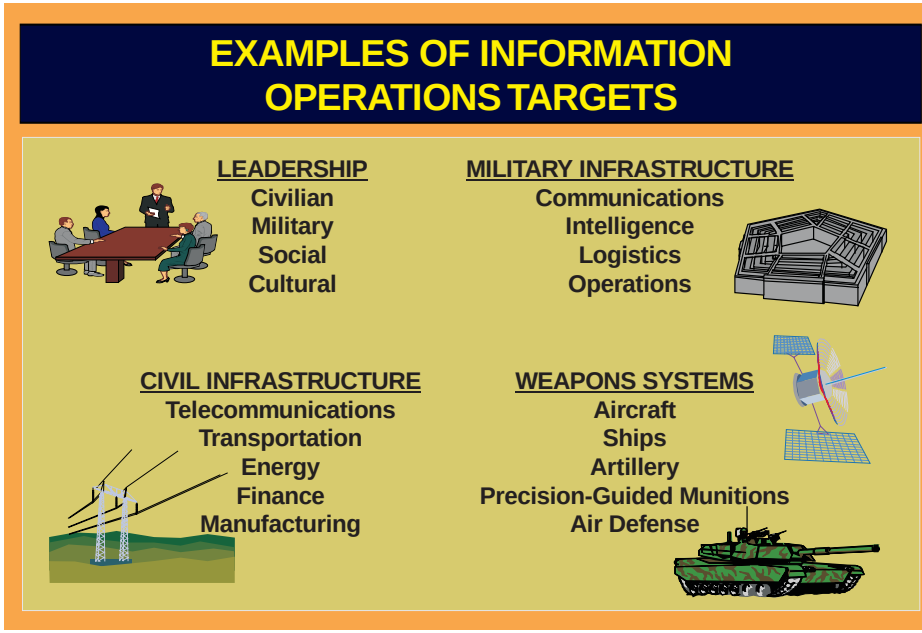


Figure I-8. Examples of Information Operations Targets

as friendly offensive capabilities may target an adversary's commercial infrastructure.

e. **Special Operations Forces Support to IO.** The unique capabilities of SOF enable the JFC to access, alter, degrade, delay, disrupt, deny, or destroy adversary information systems throughout the range of military operations and at all levels of war.

JP 3-05, "Doctrine for Joint Special Operations," provides additional guidance.

f. **Activities Related to IO.** The following activities relate to and support the conduct of IO.

- **PA seek a timely flow of information** to both external and internal audiences. Coordination of PA and IO plans is required to ensure that PA initiatives support the commander's overall objectives, consistent with the DOD principles of information. PA and IO efforts will be integrated consistent with policy or statutory limitation and security.
- The **news media** and **other information networks'** increasing availability to society's leadership, population, and infrastructure can have significant impact on national will, political direction, and national security objectives and policy.
- **CA activities are an important contributor to IO** because of their ability to interface with key organizations and individuals in the information environment. CA activities can support and assist the achievement of IO objectives by coordinating with, influencing, developing, or controlling indigenous infrastructures in foreign operational areas.

g. **Intelligence Support**

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

- **Intelligence must be timely, accurate, usable, complete, relevant, objective**, and sufficiently detailed to support an array of DOD IO requirements, to include research, development, and acquisition and operational support.

- The conduct of IO **requires unique and detailed intelligence** never before asked of intelligence collection agencies and activities. **Intelligence preparation of the battlespace** (IPB) is vital to successful IO. Support from non-DOD and non-US sources also may be required.

- **Intelligence products** must support IO planning, execution, and assessment; provide analysis of a potential adversary's IO vulnerabilities; allow determination of a potential adversary's IO capabilities and intentions; and help support the I&W process.

- **IO intelligence efforts must be focused** to provide intelligence support across the range of military operations at all levels of war. Due to the wide-spread dependence on and capability of information technologies, US military forces now depend more on individual operators at all levels to collect, process, analyze, disseminate, and act on information. Thus everyone, not just intelligence specialists, must be part of the threat assessment and response process.

- Guidance for **specific intelligence support required for offensive and defensive IO** is provided in Chapter II, "Offensive Information Operations," and Chapter III, "Defensive Information Operations," respectively.

h. **IO as an Enabler to Combatant Commanders**

- Rapidly advancing information-based technologies and an increasingly competitive global environment have thrust information into **the center stage in society, government, and warfare in the 21st Century**. Information and information-based technologies are pervasive and impact every facet of warfighting from planning, deployment, sustainment, postconflict, and redeployment processes to the plethora of forces and weapons systems employed by JFCs and their component commanders (See Figure I-9).

- **All forms of national power**, to include military operations in particular, **are dependent on many simultaneous and integrated activities** that, in turn, depend on information and information systems. This is especially true of those activities associated with critical C2 processes. Some of these activities include conducting strategic deployment, sustaining theater forces, ensuring force protection — both in garrison and in forward-deployed areas, preserving theater strategic C2, and developing strategic and theater intelligence.

- **Information itself is a strategic resource vital to national security.** This reality extends to warfighters at all levels. Increasingly complex information systems are being integrated into traditional disciplines such as mobility, logistics, and C4I.

- **IO can be used positively to reinforce common interests and objectives of multinational partners** to deter

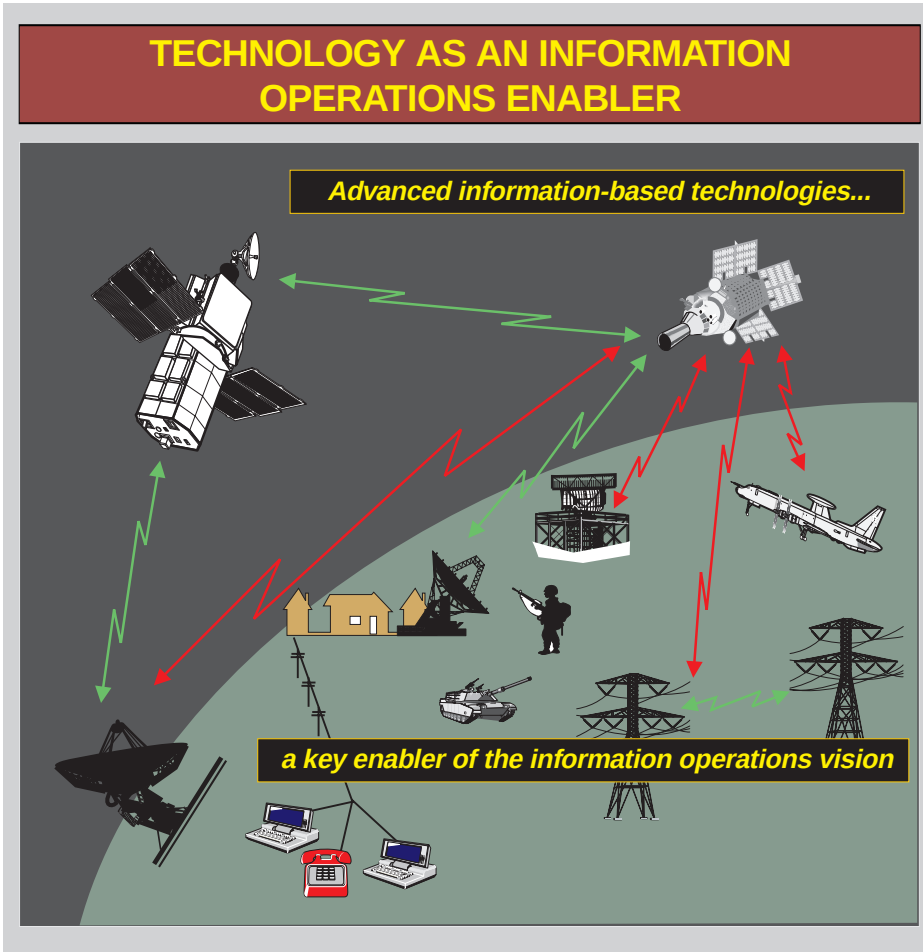


Figure I-9. Technology as an Information Operations Enabler

adversaries from initiating actions detrimental to interests of the United States or partners, or to the conduct of friendly military operations.

- If carefully conceived, coordinated, and executed, **IO will make an important contribution to combatant commanders' efforts** to defuse crises and return to peace, reduce periods of confrontation, enhance the impact of other elements of national power, and forestall or eliminate the need to employ forces in combat situations. Simultaneously, IO also must prepare the battlespace for conflict and should enhance the ability of all components to conduct successful combat operations.

"Nothing is more worthy of the attention of a good general than the endeavor to penetrate the designs of the enemy."

Niccolo Machiavelli, Discourse

INFORMATION OPERATIONS AND THE PERSIAN GULF WAR

During the Persian Gulf War, defensive information operations ensured that the Coalition soundly defeated Saddam Hussein's political strategy, which was aimed at influencing the decision making coalition nation leadership. Immediately after the invasion of Kuwait, Iraq began campaigning for public support. This effort included defaming Kuwait's ruling family and portraying Iraq as the champion of anti-colonialism, social justice, Arab unity, the Palestinian cause, and Islam. In an apparent move to defuse initial international condemnation of its invasion of Kuwait, Saddam falsely announced Iraqi troops would begin pulling out of Kuwait on 6 August 1990. In spite of Hussein's efforts to influence Coalition actions, the Coalition's information strategy ensured that the war was fought under favorable conditions that took full advantage of Coalition strengths and Iraqi weaknesses, ensuring Saddam's political and military strategy was soundly defeated. Despite Hussein's attempts to intimidate his neighbors, the Gulf States requested outside help and a Coalition formed. The Arab "street" did not rise up on his behalf, and Israeli restraint in the face of Scud attacks undermined his plan to turn the war into an Arab-Israeli conflict. Coalition leadership aggressively countered Saddam's widely publicized threats of massive casualties and his taking of hostages, neither of which deterred Coalition resolve. Saddam's attempts to take the offense by his use of Scuds and the attack on the Saudi town of Al-Khafji failed to achieve their strategic purpose of reducing the Coalition's will to fight. On all information fronts, the effective use of information operations by the Coalition to defend against Saddam's information strategy ensured that Iraq was not only beaten, but also failed to ever seize the initiative.

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

CHAPTER II
OFFENSIVE INFORMATION OPERATIONS

"Hit first! Hit hard! Keep on hitting!"

Admiral Sir John Fisher, Memories, 1919

"Information is the currency of victory on the Battlefield."

Gen. Gordon Sullivan,
Former Army C/S

1. Principles and Capabilities

There are both offensive and defensive aspects of IO. Common links between the two aspects include the target sets involved in IO and the dependence upon information to plan operations, deploy forces, and execute missions. **Offensive IO are conducted across the range of military operations at every level of war to achieve mission objectives.** The employment of IO to affect an adversary's or potential adversary's information or information systems can yield a tremendous advantage to US military forces during times of crisis and conflict. As a result, combatant commanders must carefully consider the potential of IO to deter, forestall, or resolve back crises.

a. **Principles.** Offensive IO principles include the following.

- The **human decision making processes** are the ultimate target for offensive IO. Offensive IO involve the integration and orchestration of varied capabilities and activities into a coherent, seamless plan to achieve specific objectives.

- **Offensive IO objectives** must be clearly established, support overall national and military objectives, and include identifiable indicators of success. The potential spectrum of IO objectives ranges from peace to war (See Figure II-1).

- **Selection and employment of specific offensive capabilities** against an adversary must be appropriate to the situation and consistent with US objectives. These actions must be permissible under the law of armed conflict, consistent with applicable domestic and international law, and in accordance with applicable rules of engagement.

- Offensive IO may be the **main effort**, a **supporting effort**, or a **phase** of a JFC's campaign or operation.

- Offensive IO in support of a JFC's campaign or operation may include planning and execution by non-DOD forces, agencies, or organizations and **must be thoroughly integrated, coordinated, and deconflicted** with all other aspects and elements of the supported campaign or operation.

- In order to efficiently attack adversary information and information systems, **it is necessary to be able to do the following.**

  •• Understand the adversary's or potential adversary's perspective and how it may be influenced by IO.

  •• Establish IO objectives.

  •• Identify information systems value, use, flow of information, and vulnerabilities.

Figure II-1. Examples of Information Operations Objectives

•• Identify targets that can help achieve IO objectives.

•• Determine the target set.

•• Determine the most effective capabilities for affecting the vulnerable portion of the targeted information or information systems.

•• Predict the consequences of employing specific capabilities with a predetermined level of confidence.

•• Obtain necessary approval to employ IO.

•• Identify intelligence and combat information feedback necessary to support assessment.

•• Integrate, coordinate, and implement IO.

•• Evaluate the outcome of specific IO to the predetermined level of confidence.

b. **Capabilities.** When employed as an integrating strategy, IO weave together related capabilities and activities toward satisfying a stated objective. **Offensive IO applies perception management actions** such as PSYOP, OPSEC, and military deception, and may apply attack options such as EW and physical attack/destruction **to produce a synergistic effect** against the elements of an adversary's information systems. There are many capabilities and activities that require integration both defensively and offensively to conduct successful IO. Some of these capabilities or activities appear more offensive or defensive in nature, but it is their **integration** and **potential synergy** that ensures successful offensive and defensive IO.

- **Assigned and supporting capabilities and activities** that can be integrated to conduct offensive IO include the same capabilities and processes that traditionally support C2W — OPSEC, PSYOP, military deception, EW, and physical attack/destruction. Additionally, CNA may be considered for development and integration in offensive IO.

  •• **OPSEC.** OPSEC contributes to offensive IO by **slowing the adversary's decision cycle** and providing opportunity for **easier and quicker attainment of friendly objectives**. OPSEC focuses on having a good understanding of the adversary decision maker's ability to

OPSEC IN OPERATION DESERT STORM

DESERT STORM demonstrated the effectiveness of the integrated use of OPSEC and deception to shape the beliefs of the adversary commander and achieve surprise. Deception and OPSEC efforts were combined to convince Saddam Hussein of a Coalition intent to conduct the main offensive using ground and amphibious attacks into central Kuwait, and to dismiss real indicators of the true Coalition intent to swing west of the Iraqi defenses in Kuwait and make the main attack into Iraq itself. The OPSEC planning process showed that, prior to initiation of the air offensive, Coalition force and logistic preparations for the ground offensive could not be hidden from Iraqi intelligence collection. The plan then called for conducting the preparations in areas of Saudi Arabia logical for an attack into Kuwait; using the air offensive to blind most of the Iraqi intelligence collectors, and then secretly moving the force to the west where it would be postured for the main ground offensive into Iraq. To support this, deception would create false indicators and OPSEC would alter or hide real indicators, all to help Saddam Hussein conclude the Coalition would attack directly into Kuwait. Deception measures included broadcasting tank noises over loudspeakers and deploying dummy tanks and artillery pieces as well as simulated HQ radio traffic to fake the electronic signatures of old unit locations. OPSEC measures included allowing selected Iraqi intelligence collectors to see aspects of the final Coalition preparations for the real supporting attack into Kuwait and directing aggressive patrolling in this sector. The Marine amphibious force, positioned off the coast, conducted both deception and OPSEC. While USCENTCOM hoped to use them only as a demonstration to keep the Iraqi attention fixed on Kuwait, the Marines were nonetheless a real force that could have been employed if the Iraqis had not bought the Coalition deception.

SOURCE: The Joint Staff Special Technical Operations Division

collect reliable, adequate, and timely intelligence, and, when integrated with other capabilities, shapes to our advantage the adversary's knowledge and beliefs about our operations. **OPSEC denies the adversary critical information** about friendly capabilities and intentions needed for effective and timely decision making, leaving the adversary vulnerable to other offensive capabilities. **Early integration of OPSEC into mission planning is essential** to reduce a friendly operation's revealing indicators to a minimum and better target the adversary's decision making process.

"No enterprise is more likely to succeed than one concealed from the enemy until it is ripe for execution."

Niccolo Machievelli, The Art of War, 1521

•• **PSYOP.** PSYOP are actions to **convey selected information and indicators to foreign audiences**. They are designed to influence emotions, motives, reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals. PSYOP have strategic, operational, and tactical applications, including truth projection activities that support military deception operations. (1) At the **strategic level**, PSYOP may take the form of political or diplomatic positions, announcements, or communiqués. (2) At the **operational level**, PSYOP can include the distribution of leaflets, loudspeaker broadcasts, radio and television broadcasts, and other means of transmitting information that encourage enemy forces to defect, desert, flee, or surrender. Persistent attacks can have a synergistic effect with PSYOP, accelerating the degradation of morale and further encouraging desertion. (3) At the **tactical level**, PSYOP include the use of loudspeakers and other means to promote fear or dissension in enemy ranks. (4) PSYOP forces also may shape attitudes and influence behaviors through face-to-face communication. In addition, PSYOP may support military deception operations.

JP 3-53, "Doctrine for Joint Psychological Operations," provides additional detail.

"The real target in war is the mind of the enemy commander, not the bodies of his troops."

Captain Sir Basil Liddell Hart, Thoughts on War, 1944

•• **Military Deception.** (1) Military deception, as executed by JFCs, **targets adversary decision makers through effects on their intelligence collection, analysis, and dissemination systems**. This deception requires a thorough knowledge of opponents and their decision making processes. Anticipation is key. During the formulation of the commander's concept, particular attention is placed on defining **how the JFC would like the enemy to act at critical points in the battle**. Those desired enemy actions then become the goal of deception operations. **Military deception is focused on desired behavior**, not simply to mislead thinking. The purpose is **to cause adversary commanders to form inaccurate impressions** about friendly force capabilities or intentions, misappropriate their intelligence collection assets, or fail to employ combat or support units to their best advantage. (2) Military deception operations normally are an integral element of joint operations. **Planning for military deception operations is top-down**, in the sense that subordinate deception plans support the higher level plan. (3) **Commanders at all levels can plan military deception operations.**

Plans may include the employment of lower-level units, although subordinate commanders may not know of the overall deception effort. It is therefore essential for commanders to coordinate their deception plans with their senior commander to ensure overall unity of effort. (4) **Military deception operations depend on intelligence operations** to identify appropriate deception targets, to assist in developing a credible story, to identify and focus on appropriate targets, and to assess the effectiveness of the military deception plan. (5) Military deception operations are a powerful tool in full-dimensional operations, but are **not without cost**. Forces and resources must be committed to the deception effort to make it believable, possibly to the short-term detriment of some aspects of the campaign or operation. OPSEC for military deception operations may dictate that only a select group of senior commanders and staff officers in the joint force know which actions are purely deceptive in nature. This situation can cause confusion within the force and must be closely monitored by JFCs and their staffs.

JP 3-58, "Joint Doctrine for Military Deception," provides additional detail.

"All warfare is based on deception."

Sun Tzu, The Art of War, c. 500 BC, tr. Griffith

•• **EW.** (1) The three major subdivisions of EW are **electronic attack** (EA), **electronic protection** (EP), and **electronic warfare support** (ES). All three contribute to both offensive and defensive IO. **EW** is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. **EA** involves actions taken to attack the adversary with the intent of degrading, neutralizing, or destroying adversary combat capability to prevent or reduce an adversary's effective use of the electromagnetic spectrum. **EP** involves such actions as self-protection jamming and emission control taken to protect friendly use of the electronic spectrum by minimizing the effects of friendly or adversary employment of EW that degrade, neutralize, or destroy friendly combat capability. **ES** contributes to the JFC's situational awareness by detecting, identifying, and locating sources of intentional or unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. (2) EA should be employed to **attack the enemy according to established principles of warfare**. The decision to employ EA should be based not only on overall joint campaign or operation objectives, but also on the risks of possible adversary responses and other potential effects on the campaign or operation. EP and ES routinely are conducted during peacetime as well as during periods of crisis or conflict. (3) The JFC should ensure **maximum coordination among EW and other IO intelligence and communications support activities** for maximum effect and to reduce electronic fratricide. This coordination is necessary to ensure effective exchange of information, eliminate undesirable duplication of effort, and provide mutual support.

See JP 3-51, "Electronic Warfare in Joint Military Operations," for additional detail.

•• **Physical attack/destruction** refers to the use of "hard kill" weapons against designated targets as an element of an integrated IO effort.

•• **CNA.** Guidance concerning planning and execution of CNA is

EA-6B conducting electronic warfare

provided in Appendix A, "Supplemental Information Operations Guidance," (published separately).

- Other activities that may contribute to offensive IO include, but are not limited to, **PA** and **CA**.

  •• **PA.** PA activities: (1) **Expedite the flow of accurate and timely information** to internal (own organization) and external (the public) audiences. (2) **Create an awareness** of the military goals during a campaign or operation. (3) Satisfy the desires of the internal and external audiences to be kept **informed** about the campaign or operation. (4) Inform internal and external audiences of **significant developments** affecting them. (5) Through the public media, allow a **JFC to inform** an adversary or a potential adversary about the friendly force's intent and capability. PA activities will not be used as a military deception capability or to provide disinformation to either internal or external audiences.

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

"When regard for truth has been broken down or even slightly weakened, all things remain doubtful."

Saint Augustine, On Lying

•• **CA Support to IO.** (1) CA encompass activities that military commanders take to **establish and maintain relationships** between their forces and the civil authorities and general populations, resources, and institutions in friendly, neutral, or hostile areas where their forces are employed. These activities may occur before, during, subsequent to, or in the absence of other military actions. (2) CA activities support the JFC's initiatives to **improve relations** with friendly foreign military forces and civilian populations and **regional strategy and long-term goals** by strengthening the capabilities of a host nation in effectively applying its indigenous resources to mitigate or resolve its instability, privation, or unrest. (3) **CA and PSYOP are mutually supportive within civil-military operations (CMO).** During military operations other than war (MOOTW), PSYOP support various CA activities (e.g., establish population control

measures) to gain support for the host nation (HN) government in the international community, and reduce support or resources to those destabilizing forces threatening legitimate processes of the HN government. CA personnel and forces can advise commanders on the most effective military efforts to support friendly or HN civilian welfare, security, and developmental programs, **PSYOP maximize these efforts** through information products and programs. PSYOP publicize the existence or successes of these CMO activities to generate target population confidence in and positive perception of US and HN actions.

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

•• Other classified capabilities are outlined in Appendix A, "Supplemental Information Operations Guidance," (published separately).

2. Range of Military Operations

Offensive IO may be conducted in a variety of situations and circumstances across the range of military operations and **may have their greatest impact on influencing an adversary decision maker in peacetime and the initial stages of a crisis**. **The initial IO goal is maintaining peace, defusing crisis, and deterring conflict.** As a situation or circumstance moves towards conflict, the ability to target and engage critical adversary information and information systems becomes more difficult. **If deterrence fails, all capabilities may be applied to meet the stated objectives.** As an adversary prepares for conflict, information systems may become crucial to adversary operations (See Figure II-2).

a. **MOOTW.** MOOTW are military operations that encompass the use of military capabilities across the range of military operations short of war. MOOTW can be applied to complement any combination of the other instruments of national power and occur before, during, and after war. MOOTW focus on deterring war, responding to crisis, resolving conflict, and promoting peace. Noncombat MOOTW may be conducted simultaneously with combat MOOTW, such as a foreign humanitarian assistance (FHA) operation in conjunction with a peace enforcement operation. Although MOOTW are generally conducted outside of the United States, some types may be conducted within the United States in support of civil authorities consistent with established law.

- **MOOTW Not Involving the Use or Threat of Force.** Use of military forces in peacetime helps keep the day-to-day tensions between nations below the threshold of crisis and armed conflict and maintains US influence in foreign lands. These operations, by definition, do not involve combat, but military forces always should be prepared to protect themselves and respond to a changing situation.

- **MOOTW Involving the Use or Threat of Force.** When other instruments of national power (diplomatic, economic, and informational) are unable to influence a deteriorating or potentially hostile situation, military force may be required to demonstrate US resolve and capability, support the other instruments of national power, or terminate the situation on favorable terms. The general goals of US military operations during such periods are to support national objectives, deter war, and return to a state of peace. Certain situations may require US forces to become involved in combat

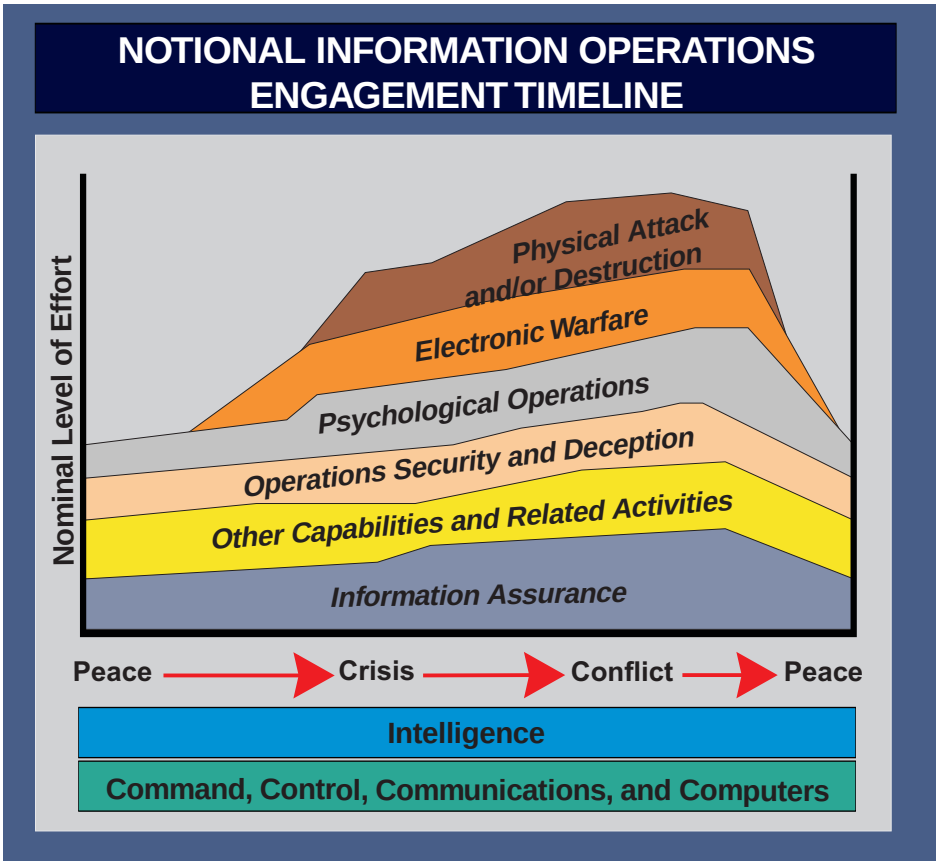


Figure II-2. Notional Information Operations Engagement Timeline

operations. MOOTW involving combat, such as peace enforcement, may have many of the same characteristics of war, including active combat operations and employment of most combat capabilities. In MOOTW, political considerations permeate all levels and the military may not be the primary player. As a result, these operations normally have more restrictive rules of engagement (ROE) than in war.

b. **War.** When other instruments of national power are unable or inappropriate to achieve national objectives or protect national interests, the US national leadership may employ military forces to conduct large-scale, sustained combat operations to achieve US objectives or protect US interests, placing the United States in a wartime state. In such cases, the goal is to win as quickly as possible, achieving national objectives and concluding hostilities on terms favorable to the United States and its multinational partners. It is possible for part of an AOR or JOA to be in a wartime state while MOOTW are being conducted elsewhere within the same AOR or JOA.

c. **IO Conducted During Peacetime**

- **Offensive IO-related plans with their associated capabilities may be employed in peacetime** to promote peace, deter crisis, control crisis escalation, or project power. The employment of offensive capabilities in these circumstances may require NCA

approval with support, coordination, deconfliction, cooperation, and/or participation by other USG departments and agencies. Military offensive IO must be integrated with other USG IO efforts to maximize synergy, to enable capabilities and activities when needed, and to prevent confusion and fratricide. To integrate offensive efforts, desired objectives should be determined and measures of IO success should be established.

- **Offensive IO objectives and measures of effectiveness will change based on the situation or circumstances**, for example, influencing a potential adversary during peacetime or conducting various MOOTW not involving the use or threat of force. Depending on the military objective and ability to accurately target and engage adversary information systems, offensive IO can be used to affect the adversary course of action (COA) or degrade the adversary's ability to respond, thereby influencing the overall goal of maintaining or returning to peace.

- **Offensive IO may be conducted in some types of MOOTW not involving the use or threat of force.** Examples of potential peacetime applications of offensive IO include employment of capabilities to disrupt drug cartel LOCs in support of drug interdiction efforts and conducting PSYOP against a belligerent's potential allies with the goal of severing external sources of military, economic, and political support. CA or PA activities may be used to support offensive IO in some cases, such as FHA or military support to civil authorities.

- Offensive IO planning in support of peacetime objectives and some types of MOOTW also must **consider and prepare the battlespace** and **set the conditions** for the successful execution of operations against an adversary in conflict.

d. **IO Conducted During Crisis and Conflict (Including War)**

- Beyond the threshold of crisis, **offensive IO can be a critical force enabler for the JFC**. Employment of offensive IO can affect every aspect of an adversary's decision cycle by impacting IO targets. In addition, offensive IO can protect information and information systems vital to the US military. Offensive IO becomes a **force multiplier** to support combat operations. Exploitation, corruption, disruption, degradation, or destruction of adversary information systems and their will to fight (human element) are the primary goals of offensive IO in war and MOOTW involving the use or threat of force.

- Offensive IO against adversary information systems and their will to fight **may not take place in the same physical battlespace or be conducted in the same time frame as the combat operations they support**, but must be synchronized thoroughly with the supported combat operations.

- Offensive IO should **help friendly forces dominate combat operations** and influence the adversary to terminate hostilities on terms favorable to the United States.

3. Levels of War

Offensive IO may be conducted at all levels of war — strategic, operational, and tactical — inside and outside the traditional military battlespace. In a combatant commander's AOR, IO normally are conducted as an integral part of a joint or multinational campaign or operation. **The**

level of war at which offensive IO are conducted normally will vary across the range of military operations and with objectives.

a. **Strategic Level**

- Offensive IO at the strategic level of war will be **directed by the NCA** and **planned in coordination with other agencies or organizations outside the Department of Defense**. This may include offensive IO conducted within a combatant commander's AOR. Such operations must be coordinated with the affected combatant commander to ensure unity of effort and prevent conflict with possible ongoing operational level IO.

- Offensive IO for strategic level objectives seek to **engage adversary or potential adversary leadership to deter crisis and end hostilities once they occur**. Potential effects of offensive IO can be widespread or targeted at a narrow range of adversary capabilities. As such, these operations may be conducted to influence or affect all elements (political, military, economic, informational) of an adversary's national power.

- **IO may be used to effectively attack strategic targets**, while minimizing potentially devastating social, economic, and political effects normally associated with conventional military operations. Such IO continue to increase in importance in the post Cold-war era.

- Offensive IO in support of strategic security objectives and guidance **may be conducted or planned by a combatant or subordinate commander within an assigned AOR** as a result of tasking by the NCA. These IO normally would be integrated with any ongoing offensive or defensive IO at the strategic or operational levels being planned and/or conducted by the affected combatant commander.

- When effectively integrated and executed in combatant command campaign plans and/or OPLANs/operation orders (OPORDs), **strategic-level offensive IO degrade an adversary's leadership ability** to effectively execute campaigns or operations and contribute to achieving information superiority of friendly forces in the AOR.

b. **Operational Level**

- Offensive IO at the operational level of war normally are **conducted by a combatant commander within the assigned AOR, or the combatant commander may assign that responsibility to a subordinate commander**. Offensive IO at this level will involve the use of military forces to achieve strategic objectives through the design, organization, integration, and conduct of strategies, campaigns, and operations. In MOOTW, most offensive IO are conducted at the operational level of war.

- Offensive IO at the operational level of war will **focus on an adversary or potential adversary in the combatant commander's AOR**. These offensive IO focus on maintaining peace, deterring crises, and, failing deterrence, on supporting quick resolution of hostilities on terms favorable to the United States. **Offensive IO at the operational level of war can have strategic value** by demonstrating US resolve to uphold and support certain democratic or human rights, values, or issues. Other combatant commanders may be tasked to conduct strategic and operational offensive IO as supporting commanders.

- h **peacetime**, operational-level offensive IO may support forward presence operations, serve as a deterrent, provide general situational awareness, assist in the development of operational assessments and estimates, and support contingency operations. In **crisis and conflict** (to include war), continuous engagement in offensive IO may help the JFC seize and sustain the initiative and synchronize operational capabilities.

- Combatant commanders may task **subordinate JFCs to plan and conduct offensive IO at the operational level.** Normally, these taskings would be passed to commanders of subordinate unified commands and joint task forces (JTFs). When subordinate JFCs are tasked to plan and conduct offensive IO at this level of war, the tasking authority must ensure appropriate offensive capabilities or activities are either resident in the assigned or attached forces or are made available to the subordinate JFCs for both planning and execution.

c. **Tactical Level**

- Offensive IO at the tactical level of war may be conducted by a **Service or functional component commander** under a subordinate unified command or JTF, by a subordinate JTF, or by a **single-Service force** reporting directly to the JFC.

- While commanders use all aspects of offensive IO at the tactical level of war, the primary focus of offensive IO at this level is **to deny, disrupt, destroy, or otherwise control an adversary's use of information and information systems**. A JFC may rely more heavily on EW and physical attack/destruction to handle targets relating to C2, intelligence, and other critical information-based processes directly related to conducting military operations.

- As in strategic and operational offensive IO, the human element is **also the focus of offensive IO at the tactical level of war.** Targeting the human element attempts to affect the will of an adversary's military forces to resist and to deny an adversary's use of the affected populace for advantageous purposes. These offensive IO ensure the affected populace is kept abreast of friendly purposes and intent, adversary actions harmful to the interest and well being of the populace, and other information that will favorably influence the populace with respect to US goals and interests in the AOR or JOA.

4. Intelligence and Information Systems Support

a. **Intelligence Support to Offensive IO**

- **General. Offensive IO require broad-based, dedicated intelligence support.** Because intelligence support to offensive IO may require significant lead time and the effectiveness of many offensive capabilities is significantly improved by early employment, **potential intelligence collection sources and access should be developed as early as possible**. Significant lead time often is required to fulfill offensive IO requirements. Appropriate assessment procedures to support IO should be developed and established. Figure II-3 provides a sequential overview of the relationship between offensive IO and required intelligence support.

- **Sources.** To plan and execute offensive IO, intelligence must be collected, stored, analyzed, and easily retrieved, especially for offensive IO supporting short-notice

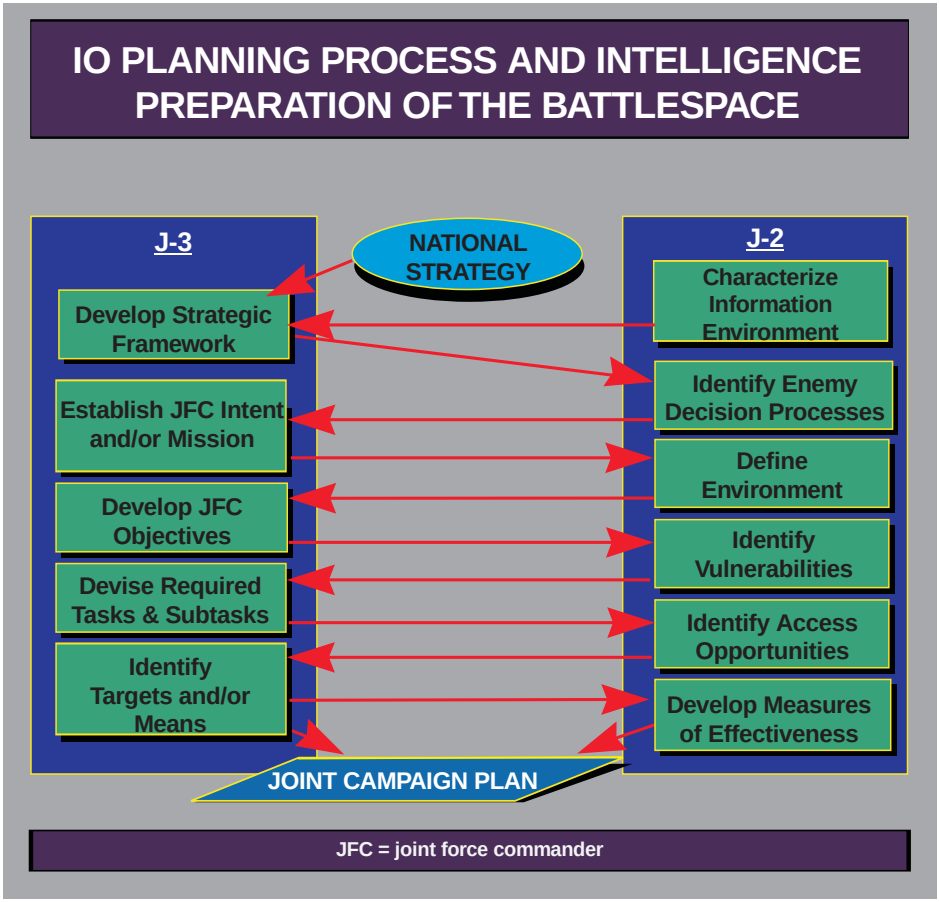


Figure II-3. IO Planning Process and Intelligence Preparation of the Battlespace

contingencies. **Intelligence collection for offensive IO includes all possible sources**, from national-level covert operations through local open sources such as news media, commercial world contacts, academia, and local nationals. Rapid processing, analysis, and dissemination of all-source data will reinforce and confirm relevant IO information and intelligence and enable the targeting and exploitation of an adversary's critical capabilities, systems, and facilities. Other intelligence sources and collection means, such as the INTERNET, commercial publications, and commercial radio, should be employed as required.

- **IPB.** For offensive IO, **IPB is the continuous process used to develop a detailed knowledge of the adversary use of information and information systems**. IPB for offensive IO uses a process of overlapping and simultaneous actions that produces situation updates, thereby providing JFCs and their subordinate commanders with flexible offensive IO options. IPB in support of offensive IO builds upon traditional combat IPB and requires the following.

  •• Knowledge of the technical requirements of a wide array of information systems.

•• Knowledge of the political, economic, social, and cultural influences.

•• The ability to develop templates used to portray the battlespace and refine targets and methods for offensive IO COAs.

•• An understanding of the adversary's or potential adversary's decision making process.

•• An in-depth understanding of the biographical background of key adversary leaders, decision makers, communicators, and their advisors, to include motivating factors and leadership style.

•• Knowledge of AOR/JOA geographic, atmospheric, and littoral influences on adversary and friendly operations.

See JP 2-01.3, "Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace," for further guidance.

b. **Information Systems Support to Offensive IO**

- Information systems **collect, transport, process, disseminate, and display information used to support offensive IO.** These systems enable JFCs and their component commanders to use information effectively to maintain an accurate view of the battlespace and to plan and execute offensive IO.

- Information systems also **provide JFCs and their subordinate JFCs with a means to interface with the GII** in a manner that maximizes the scope and measures the effectiveness of offensive IO.

- Finally, information systems support offensive IO by **providing the global reach capability** that allows NCA, combatant command, subordinate joint force, and component synchronization, coordination, and deconfliction of offensive IO across the range of military operations at all levels of war.

5. Offensive IO Targeting

a. **General**

- **Offensive IO can be effective against all elements of national power.** Offensive IO targeting, as an integral element of the combatant commander's approved plan and targeting strategy, should consider all elements of the adversary's national power to determine how best to achieve desired objectives.

- Offensive IO can target human decision processes (human factors), the information and information systems used to support decision making (links), and the information and information systems used to process information and implement decisions (nodes). **Offensive IO efforts should examine all three target areas to maximize opportunity for success.** The selection of offensive IO targets must be consistent with US objectives and applicable international conventions and ROE (See Figure II-4).

- **The IO cell** explained in Chapter IV, "Information Operations Organization," **will be a major source of information for the JFC targeting process** that normally culminates with input to the joint targeting coordination board (JTCB), if designated. IO cell representation on the JTCB should provide the conduit for ensuring effective

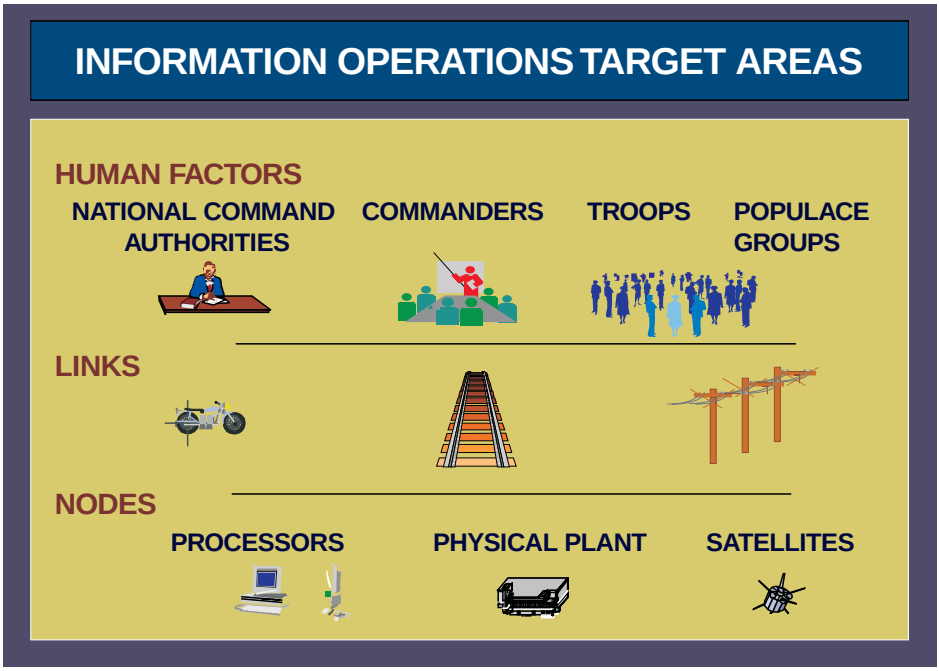


Figure II-4. Information Operations Target Areas

coordination and deconfliction of IO with other ongoing operations.

- **The potential gain or loss of intelligence should be addressed in the IO targeting process.** A target's relative value as a source of intelligence must be weighed against the operational requirement for its damage or destruction. Exploitation benefits may far outweigh operational benefits. Targets may be isolated, neutralized, or bypassed, thereby supporting the operational scheme of maneuver while preserving the target as an intelligence source.

b. **Strategic.** Although strategic offensive IO targeting may involve direct, indirect, and supporting attacks, **most strategic targeting will involve direct attacks on the information and information systems** within the elements of national power that will cause an adversary or potential adversary to make decisions favorable to US interests.

c. **Operational. Operational targeting** involves timely execution of IO targeting for both **initial IO objectives** and **follow-on attacks of IO targets** based on assessment, or to support defensive IO. Surprise and security are critical to successful initial offensive IO targeting since adversary foreknowledge or source compromise may negate the initial offensive IO targeting effort. JFCs should coordinate and synchronize capabilities to execute initial offensive IO targeting in a highly responsive manner.

d. **Tactical. High-tempo operations may require rapid response to requests for follow-on attack of offensive IO targets** based on assessment conducted by national, theater, or subordinate joint force assets. **JFCs must be prepared to quickly employ offensive capabilities** in response

to requests for such follow-on attacks. Offensive IO also may need to rapidly respond to requests for attacks against adversary capabilities targeting friendly information and information systems, thereby completing a vital link between offensive and defensive IO.

"Iraq lost the war before it even began. This was a war of intelligence, EW, command and control, and counterintelligence. Iraqi troops were blinded and deafened . . . Modern war can be won by informatika and that is now vital for both the US and USSR"

Lieutenant General S. Bogdanov, Chief of the General Staff Center for Operational and Strategic Studies, October 1991

Intentionally Blank

CHAPTER III
DEFENSIVE INFORMATION OPERATIONS

"We have evidence that a large number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks on military-related computers."

John M. Deutsch, Director, CIA
Washington Post, 26 June 1996

1. General

JFCs depend upon information to plan operations, deploy forces, and execute missions. Information systems serve as enablers and enhance warfighting capabilities; however, increasing dependence upon rapidly evolving technologies makes joint forces more vulnerable. Since it is a practical impossibility to defend every aspect of our infrastructure and every information process, **defensive IO ensure the necessary protection and defense of information and information systems** upon which joint forces depend to conduct operations and achieve objectives. Four interrelated processes comprise defensive IO: **information environment protection**, **attack detection**, **capability restoration**, and **attack response**. Offensive actions play an integral role in the defensive process in that they can deter adversary intent to employ IO and/or neutralize adversary capabilities. The defensive IO processes integrate all available capabilities to ensure defense in depth. **Fully integrated offensive and defensive components of IO is essential.** This chapter describes defensive IO and supporting capabilities.

a. **Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology** to protect and defend information and information systems. Defensive IO are conducted through IA, INFOSEC, physical security, OPSEC, counterdeception, counter-propaganda, CI, EW, and SIO. Defensive IO are supported by intelligence and tailored, multi-source I&W.

b. **Defensive IO integrate and coordinate protection and defense of information and information systems** (which include C4 systems, sensors, weapon systems, infrastructure systems, and decision makers). Defensive IO are an integral part of overall force protection. Figure III-1 identifies IO information and information systems vulnerabilities.

c. **IA protects and defends information and information systems** by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IA employs technologies and processes such as multilevel security, access controls, secure network servers, and intrusion detection software (See Figure III-2).

d. **Defensive IO Integration.** Defensive IO efforts should be integrated in all military operations, to include activities by other government and nongovernment agencies or organizations operating in the JFC's AOR or JOA. **JFCs should ensure the defensive IO effort is adapted to and remains integrated with the changing information environment.** Resource allocation should be continually re-evaluated. A static defensive IO plan may become less effective if not monitored and

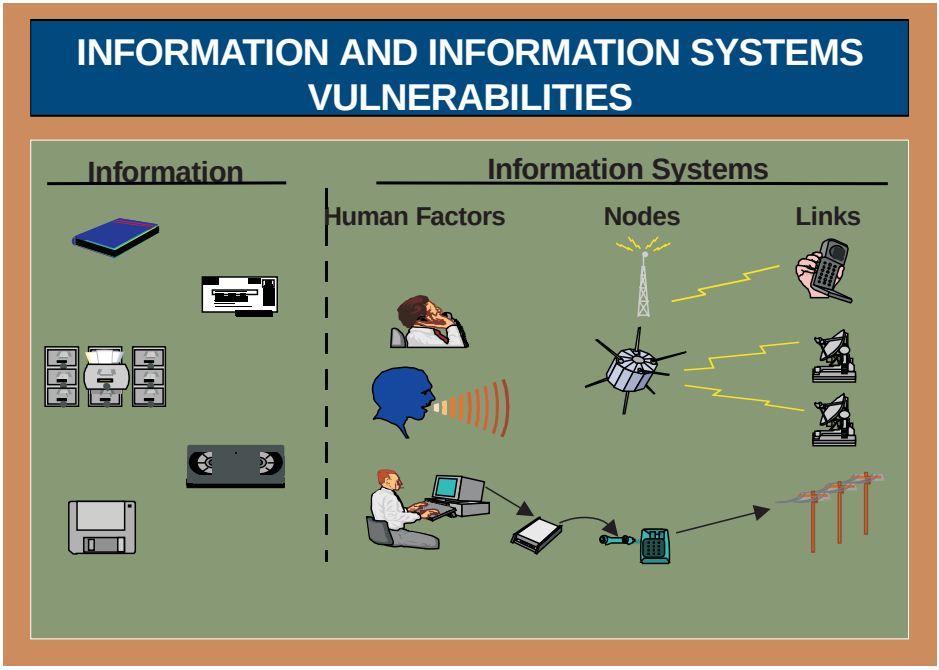


Figure III-1. Information and Information Systems Vulnerabilities

modified to continue to support JFC objectives. Continuous assessments allow the commander to adapt the defensive IO plan to the offensive IO plan and provide the framework for integrating defensive IO with offensive IO.

- **Defensive IO Integration With Offensive IO.** Defensive IO must be integrated with offensive IO to provide a timely response against identified and potential threats to friendly information and information systems. **The IO cell**

Computer information vulnerability

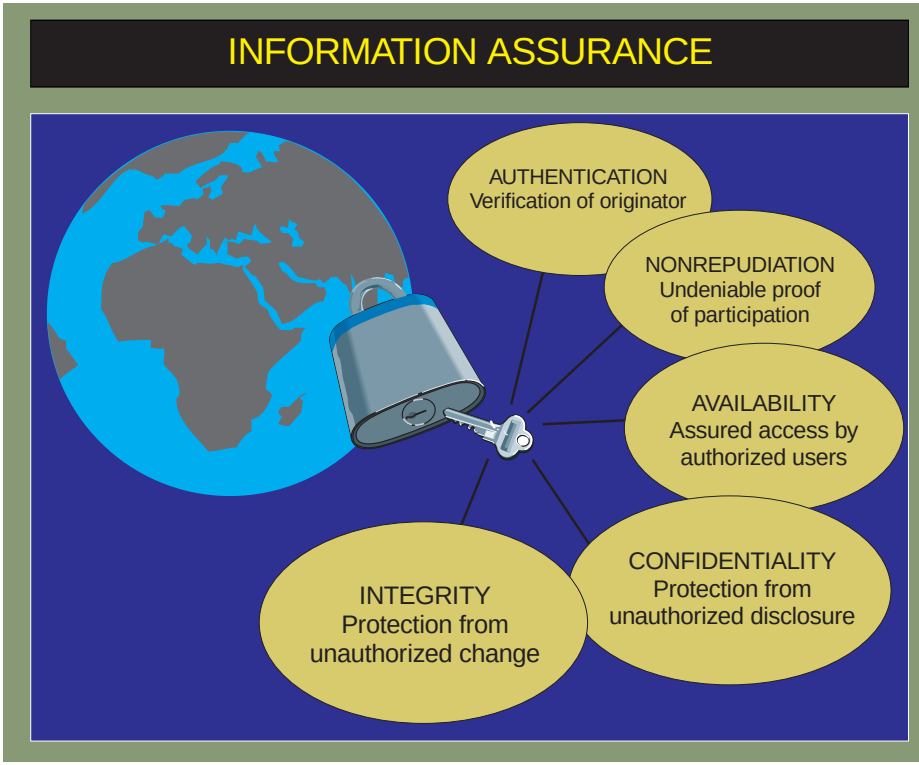


Figure III-2. Information Assurance

integrates defensive IO and offensive IO for commanders. Subordinate JFCs should ensure supporting OPLANs and OPORDs make provisions for this integration.

- **Defensive IO Integration Within a Joint Force.** Defensive IO integration within a joint force is necessary to ensure **protection**, **detection**, **restoration**, and **response** and their interrelationships are uniformly understood and practiced. In addition, defensive IO integration ensures employment of the most appropriate joint force IO response capabilities. The JFC is responsible for integrating defensive IO.

- **Defensive IO Integration Within a Multinational Force.** Information-based technology, weapons systems, intelligence, and other capabilities are often **shared, integrated, and synchronized into multinational operations to enhance operations**. While providing benefits to multinational operations, the integration of US and allied or coalition information, information-based processes, and information systems creates **additional vulnerabilities** which an adversary can exploit using IO.

•• **The JFC is the focal point** for integrating US IO in multinational operations.

•• The JFC will **establish procedures for sharing information** with multinational forces without compromising classified US intelligence, intelligence sources, or information and information systems.

•• The JFC **may consider sharing** threat data, vulnerabilities, targeting and battle damage assessment, and capabilities that could help mitigate vulnerabilities.

See JP 3-16, "Joint Doctrine for Multinational Operations," for additional guidance.

- **Levels of War.** Defensive IO require **close cooperation between military and nonmilitary organizations** internal and external to the supported JFC at all levels of war.

•• Defensive IO efforts at all levels of war should be synchronized to support all phases of a military operation.

•• To ensure unity of effort, defensive IO at all levels of war should be synchronized with planned or ongoing offensive IO.

2. The Defensive IO Process

Figure III-3 provides an **overview of the defensive IO process** and is a model scaleable to all levels of war. JFCs and their subordinate commanders should plan, exercise, and employ available capabilities and activities to support integrated defensive IO. The remainder of this chapter describes the defensive IO process and the capabilities and related activities that support it. These defensive IO capabilities and related activities include the following.

a. **OPSEC.** OPSEC is a process of **identifying critical 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 adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful; and select

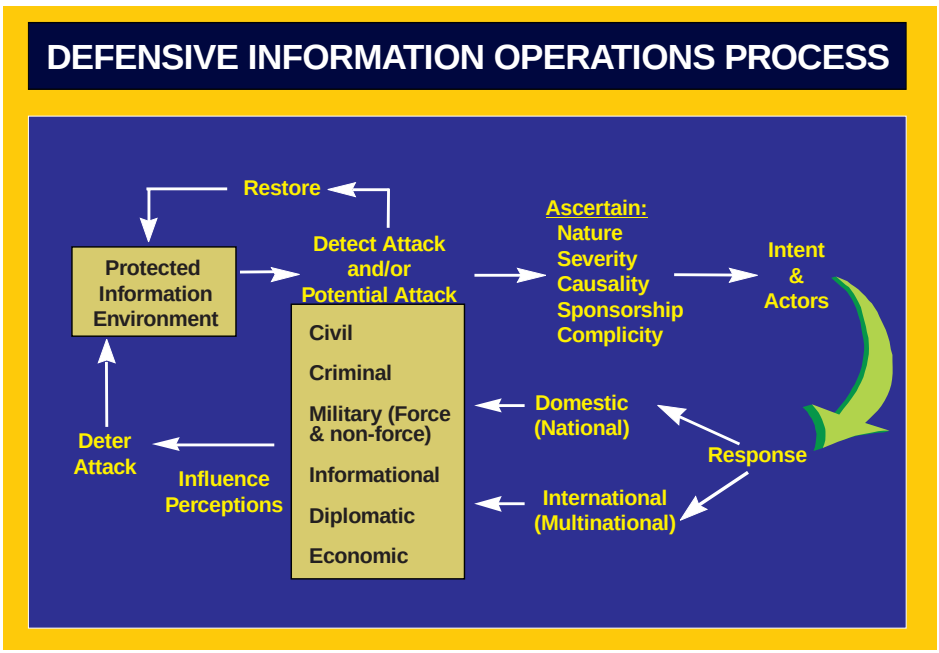


Figure III-3. Defensive Information Operations Process

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

- History has shown the **value and need for reliable, adequate, and timely intelligence**, and the harm that results from its inaccuracies and absence. It is therefore vital and advantageous to deny the adversary commanders the critical information they need and cause them to derive inaccurate, untimely analyses that influence their actions.

> *"Combat intelligence is the term applied to information of enemy forces, strength, disposition and probable movements. With personnel now assigned to Combat Intelligence, institute rigorous, continuous examination of enemy capabilities and potentialities, thereby getting the utmost value of information of the enemy and enabling our forces to be used with the greatest effectiveness. It is particularly important to comprehend the enemy point of view in all aspects."*
>
> **ADM Ernest J. King**
> **Fleet Admiral King:**
> **A Naval Record, 1952**

- **OPSEC's most important characteristic is that it is a process.** OPSEC is not a collection of specific rules and instructions that can be applied to every operation. **It is a methodology that can be applied to any operation or activity** for the purpose of denying critical information to the enemy. OPSEC is applied to all military activities at all levels of command. **The JFC should provide OPSEC planning guidance to the staff** at the time of the commander's intent and, subsequently, to supporting commanders in the chain of command. By maintaining liaison and coordinating the OPSEC planning guidance, the JFC will ensure unity of effort in gaining and maintaining the essential secrecy considered necessary for success.

JP 3-54, "Joint Doctrine for Operations Security," provides additional detail.

b. **EW.** EA, EP, and ES are examples of **EW capabilities contributing to protection and defense of information and information systems.** Related activities include changing call signs or words and frequencies and are examples of procedures or activities directly contributing to information and information systems protection. Still other activities may include frequency management and counters to attacks against force radio frequency, electro-optical, and infrared.

c. **Education, Training, and Awareness.** A key element of information environment protection is **education and training of joint force systems users, administrators, and managers.** Awareness heightens threat appreciation and the importance of adhering to joint force protective measures. Education provides the concepts and knowledge to develop appropriate policies, procedures, and operations to protect joint force information systems. Training develops the skills and abilities required to operate while mitigating joint force vulnerabilities. JFCs should develop and provide information environment education, training, and awareness materials for their staffs and components.

d. **Intelligence Support.** A critical component of intelligence support is **identifying the IO threat**. Threat information is a primary input to risk management and directly contributes to information environment protection.

- **Threat.** Intelligence provides an understanding of the threat to information and information systems by identifying potential information adversaries, their

intent, and their known and assessed capabilities.

- **Potential threats** include foreign, domestic, overt, and covert attempts to exploit friendly information or information systems. While domestic threats may be a counterintelligence issue, they are handled via law enforcement channels in accordance with intelligence oversight regulations (See Figure III-4).

- Intelligence can provide JFCs with the necessary information to **conduct threat assessments** and **develop risk management options** to mitigate their vulnerabilities.

- Threat assessment is a **continuous process** and reflects changes in the operating environment, technology, and overall threat assessment.

e. **Counterdeception.** Counterdeception supports defensive IO by negating, neutralizing, or diminishing the effects of — or gaining advantage from — a foreign deception operation. Activities contributing to awareness of **adversary posture and**

Figure III-4. Growing Threats to Information and Information Systems

intent also serve to identify adversary attempts to deceive friendly forces.

f. **Counter-propaganda Operations.** Activities identifying **adversary propaganda** contribute to situational awareness and serve to expose adversary attempts to influence friendly populations and military forces.

g. **CI.** CI activities contribute to defensive IO by **providing information** and **conducting activities** to protect and defend friendly information and information systems against espionage, sabotage, or terrorist activities.

See JP 2-01.2, "Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations," for additional guidance.

h. **PA.** PA programs contribute to information assurance by **disseminating factual information**. Factual information dissemination counters adversary deception and propaganda.

i. **Command Information.** Command information programs serve the **same purpose as PA** with respect to defensive IO. Command information programs normally are found within joint force components and at the lower level units where there is no designated PA program.

j. **Offensive IO Support.** Offensive IO can be conducted to support defensive IO throughout the range of military operations. **Offensive IO must be integrated with defensive IO** to provide timely response against identified and potential threats to friendly information and information systems.

- **Offensive IO.** Offensive IO may **neutralize adversary** capabilities prior to their employment or in response to adversary IO capabilities employed against friendly information or information systems. These offensive IO rely on timely intelligence of adversary capabilities and intentions and are proactive in nature.

- **Selection and Employment.** Selection and employment of specific offensive capabilities must be consistent with US objectives, applicable international conventions, domestic and international laws, and ROE.

3. Information Environment Protection

Defining joint force needs and dependencies is the focus of protecting the information environment. The protected information environment is bounded by what is critical to joint force operations. Information environment protection controls access to or mitigates the potential effect of adversary access to friendly information systems. **Planners should analyze information systems** to determine vulnerabilities to realistic threats, considering both military and nonmilitary systems and coordinating the efforts to reduce risks inherent in nonmilitary information systems.

a. The protected information environment is a combination of **information systems and facilities**, as well as abstract processes such as intelligence collection, analysis and production, and dissemination and integration.

b. The protected information environment is rooted in a **sound approach to managing risk**. Risk management anticipates needs in all defensive IO and **includes planning for both protection and response** based on a consideration of information needs, the value of information that may be compromised or lost if the protected information environment is breached (loss of access control), information systems vulnerabilities, threats posed by potential adversaries and natural phenomena, and resources available for

protection and defense. In addition, the value of information can change from one phase of a military operation to the next and must be considered in risk management. The elements required to accomplish JFC objectives should be included in the protected information environment.

c. The protected information environment not only **provides the degree of protection** commensurate with the value of its contents, but also **ensures capabilities** are in place to respond to a broad range of attacks.

d. **Information environment protection applies to any information medium or form**, including hard copy (message, letter, FAX), electronic, magnetic, video, imagery, voice, telegraph, computer, and human. Information environment protection involves **determining the scope** (what to protect based on the value of the information) **and the standards for protection** (to what extent through operations and the application of protective measures and technologies) (See Figure III-5). Information environment protection should reflect the changing value of information during each operational phase.

e. **JFCs should establish a protected information environment** through development of common policies, procedures, incorporation of technological capabilities, and focusing operations, to include defensive IO objectives.

- **Policies.** JFCs must augment standing defensive IO policies with **joint force-specific policies** to provide integrated and focused information environment protection tailored to their specific AORs or JOAs. These policies should address vulnerabilities and threats, friendly force capabilities, and commercial infrastructure dependencies and vulnerabilities that impact the various phases of an operation.

- **Procedures.** Joint force procedures to implement the information environment

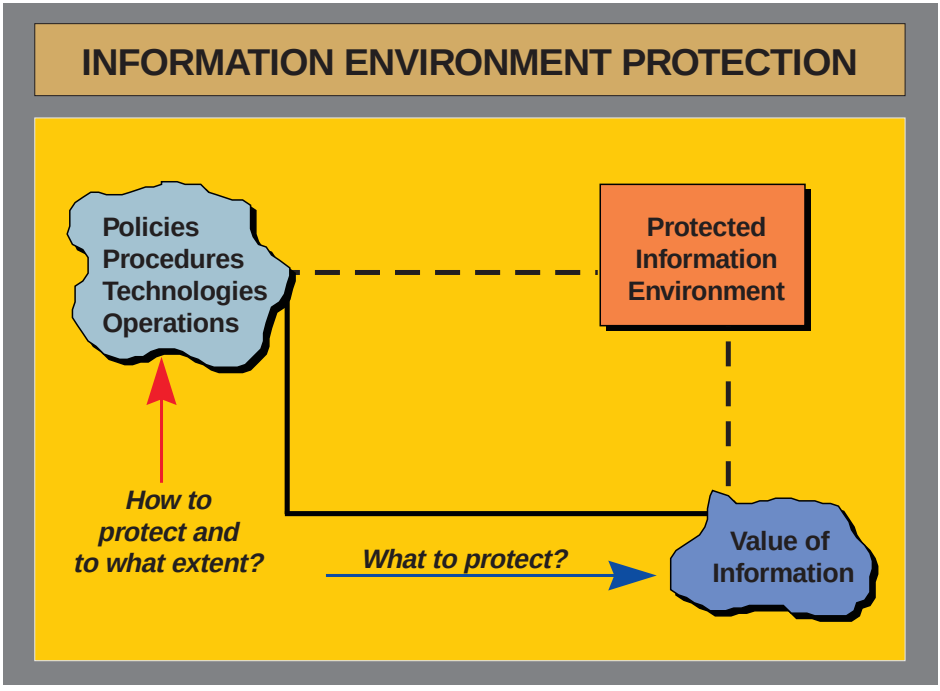


Figure III-5. Information Environment Protection

protection policies should **employ commonality** to the greatest extent possible. Use of common procedures will help achieve secure interoperability between joint force components.

- **Capabilities and Related Activities.** The following capabilities and related activities contribute to establishing the protected information environment.

  •• **Other Security Measures.** Personnel security, industrial security, and physical security measures are examples of procedures contributing indirectly to information assurance.

  •• **Vulnerability Analysis and Assessments.** Joint forces should conduct vulnerability analyses and assessments to **identify vulnerabilities** in information systems and to **provide an overall assessment** of system security posture. Integrating vulnerability analysis capabilities into joint training, exercises, and M&S helps identify and mitigate vulnerabilities and directly contributes to information environment protection. (1) Foreign and internal threats are only a part of the overall threat to information systems. **Internal threats** from malicious (disgruntled workers) and **accidental** (magnetic emanations or electrical impulses) **sources** and **natural phenomena** such as sunspots, hurricanes, tornadoes, earthquakes, and floods are significant concerns. Vulnerability analysis of systems must include consideration of these factors. (2) Vulnerability analysis and assessment efforts **focus on specific types of information systems**. For example, DISA operates a program known as the Vulnerability Analysis and Assessment Program specifically focusing on automated information systems (AIS) vulnerabilities. NSA has a communications security (COMSEC) monitoring program that focuses on telecommunications systems using wire and electronic communications. (3) **CI, personnel, physical, and facility security surveys** are additional measures designed to determine and probe organizational IO vulnerabilities. Coordinated application of all these activities provides the organization a more complete vulnerability assessment and assists in risk management.

  •• **Activities and Technologies Supporting IA.** JFCs should ensure that IA capabilities that protect and defend information and information systems are **integrated into C4 systems** and are **thoroughly tested** in joint exercises, training events, and M&S. Supporting technologies include security measures such as INFOSEC devices. (1) **INFOSEC.** INFOSEC is the protection and defense 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. INFOSEC includes those measures necessary to detect, document, and counter such threats. (2) INFOSEC is composed of computer security (COMPUSEC) and COMSEC. (a) **COMPUSEC.** COMPUSEC involves the measures and controls ensuring confidentiality, integrity, and availability of information processed and stored by a computer. These include policies, procedures, and the hardware and software tools necessary to protect and defend computer systems and information. (b) **COMSEC.** COMSEC includes measures taken to deny unauthorized persons information derived from telecommunications. COMSEC ensures telecommunications authenticity. COMSEC includes

cryptosecurity, transmission security, emission security, and physical security of COMSEC materials and information.

"In war, the defensive exists mainly that the offensive may act more freely."

Rear Admiral Alfred Thayer Mahan, Naval Strategy, 1911

4. IO Attack Detection

Timely attack detection and reporting are the keys to initiating capability restoration and attack response. Determination and/or identification of adversary or potential adversary capabilities (such as EW and military deception) and their potential to affect friendly information and information systems play critical roles in capability restoration and attack response. Elements of IO attack detection include, but are not limited to, the following.

a. **Information Warfare Centers.** The Service information warfare centers (Fleet Information Warfare Center, Air Force Information Warfare Center, and Land Information Warfare Activity) receive reports of CNA, issue warning reports, prepare and implement technical responses, coordinate restoration strategies, and prepare and issue analyses and reports.

b. **Information Systems Developers.** Information systems developers help ensure systems, particularly AISs, are designed and fielded in a manner that mitigates potential technological, employment, or integration vulnerabilities. AIS design should include automatic detection, mitigation, and reporting mechanisms.

c. **Information Systems Providers and Systems Administrators.** Increasingly powerful information systems attack techniques are continuing to emerge. Providers and administrators should recognize abnormalities in system functioning and be able to take appropriate action to report and mitigate the effects of adversary actions. They also should establish a routine for periodic risk assessment and detection or mitigation system updates.

d. **Information and Information Systems Users.** Users should be aware of potential threats to and vulnerabilities inherent in information systems. This includes recognizing abnormalities or unexplained changes in content or disturbed information and employing procedures for reporting incidents and safeguarding evidence.

e. **Law Enforcement.** Intentional information systems incidents or intrusions should be reported to military criminal investigators and counterintelligence agents to coordinate appropriate action. The resulting investigations help support systems administrators, the intelligence community, systems developers, and, as necessary, the producers and users of affected information or information systems. Internal procedures should facilitate criminal or counterintelligence investigation of the incident while protecting the integrity of the information or information systems as well as protecting individual privacy rights.

f. **Intelligence.** Intelligence contributes to attack detection by providing warning and assessment of potential adversary activity and cueing collection to specific activity indicators. Close coordination is required between intelligence, counterintelligence, law enforcement, systems developers, providers, administrators, and users to ensure timely sharing of relevant information.

- **I&W.** I&W are those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied/coalition military, political, or

Coordination of I&W is crucial to operations

economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied/coalition nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. I&W for IO are provided by the National and DOD Warning Systems. Strategic I&W provides assessments of the level of threat posed by potential adversaries' IO-related activities.

- **Defending against IO**, whether it is an adversary's deception or propaganda, or IO conducted against a JFC's intelligence data base, an automated component of the commercial national power grid, or a satellite ground station, **is predicated on how well the intelligence processes function** and on the agility of systems providers, users, and administrators to implement protective countermeasures.

- In defensive IO, the strategic I&W process analyzes adversary intent, capabilities, history, opportunity, and targeting to **assess the IO threat** to provide sufficient warning to allow for actions to preempt, counter, or otherwise moderate their effect (See Figure III-6).

- **Subordinate joint force I&W support to defensive IO** relies on indicators from sources internal and external to the Department of Defense. Joint forces should continue to analyze traditional attack indicators until a comprehensive national I&W process is established that reflects the unique characteristics of IO. Traditional indicators include, but are not limited to, the following.

  •• Adversary or potential adversary capabilities.

  •• Adversary or potential adversary intentions, preparations, deployments and related activities, and possible methods of IO attack.

  •• Adversary motivations, goals, and objectives.

  •• Changes in adversary force dispositions, military and nonmilitary activities to conduct IO, and mobilization status.

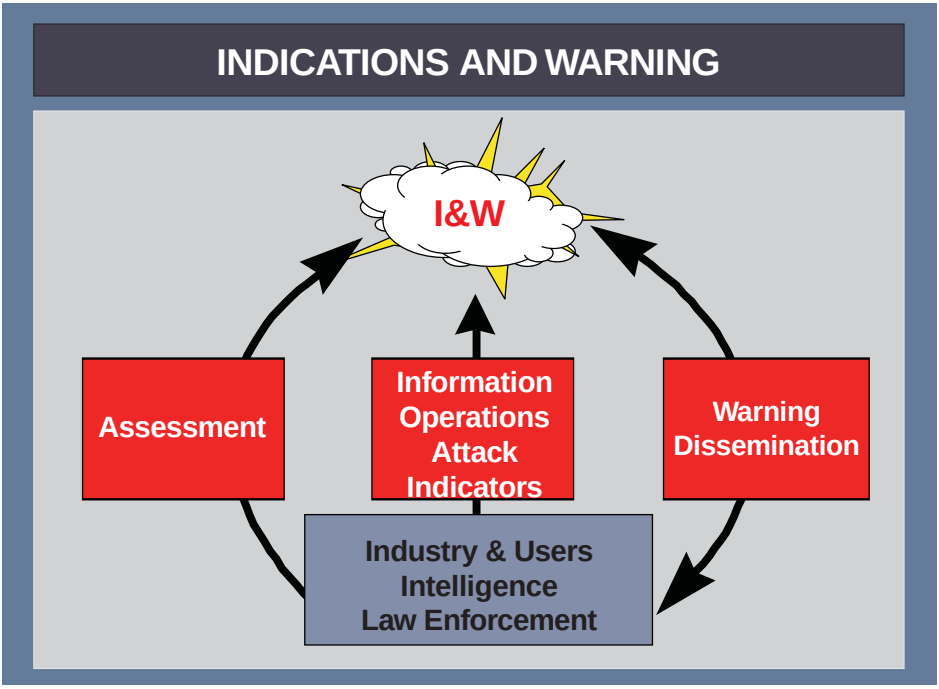


Figure III-6. Indications and Warning

•• Required adversary mobilization preparations prior to military or nonmilitary IO taking place.

g. **Reporting Structure.** Information systems designed to alert managers and administrators at all levels of abnormalities help contribute to attack detection. **Timely collation, correlation, information analysis, and warning dissemination requires a continuously functioning reporting structure.** A reporting structure linked to intelligence, counterintelligence, law enforcement, policy makers, and the information systems community, both government and commercial, is essential to defensive IO.

5. Capability Restoration

Capability restoration relies on established procedures and mechanisms for **prioritized restoration of essential functions**. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer. Information system design and modification should consider **incorporating automated restoration capabilities and other redundancy options**. A collaborative effort among government, industry, and society is required (See Figure III-7).

a. **Computer Emergency Response Teams (CERTs).** CERTs are teams composed of **personnel with technical expertise and organic equipment** that may deploy to assist remote sites in the restoration of computer services. Services have formed CERTs for **rapid response to deployed Service forces**. Some combatant commanders have formed CERTs for similar response to subordinate joint forces within their combatant command AORs. In addition, DISA can deploy CERTs to AORs or JOAs in response to specific requests for this capability. **Service components submit requests for own Service CERTs** through the administrative control line of authority. Requests for CERTs

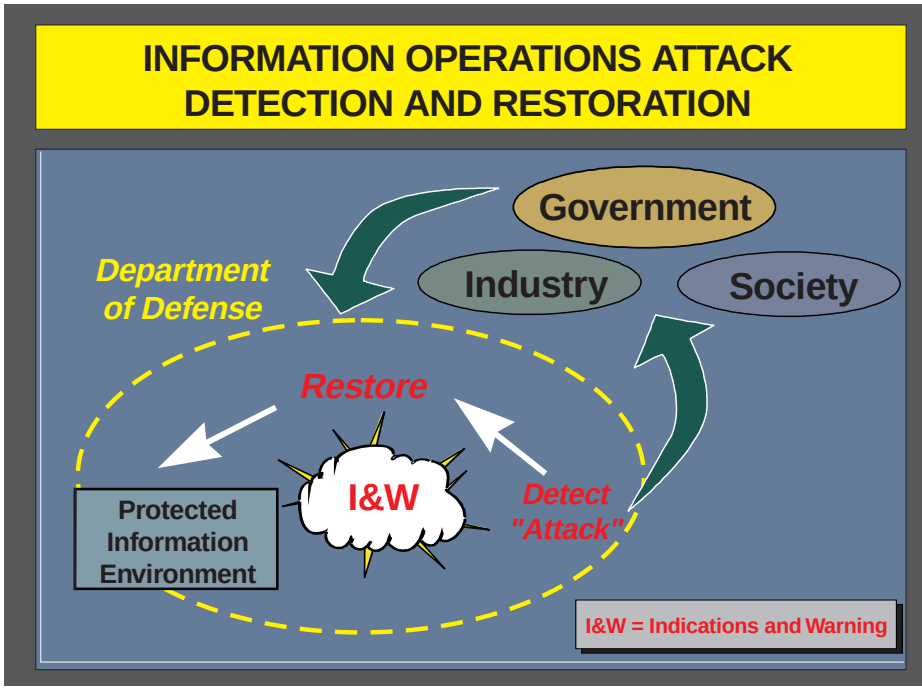


Figure III-7. Information Operations Attack Detection and Restoration

from DISA should be submitted through the supported combatant commander.

b. **Technical Restoration Capabilities.** In some cases, required technical restoration capabilities are beyond the abilities of the affected sites. **On-line** or **deployable restoration assistance** capabilities can provide required expertise and tools to restore services. In addition to CERTs, there are security incident response centers. These capabilities exist at DISA and the Services and also are available from commercial sources.

c. **Automated Intrusion Detection Systems.** Automated intrusion detection systems **provide managers and administrators with enhanced situational awareness** and **create decision points**. Immediate termination of adversary information systems access to protect against further actions and information exploitation should be weighed against the needs of the law enforcement and intelligence communities to collect against and exploit the adversary. Information systems owners and/or designated approving authorities should seek **higher authority approval** before allowing an intruder to maintain access for purposes of gathering information to support IO response. The decision relies on a risk assessment of continued access, consideration of current and future operations, and intelligence impact.

d. **Inventory of Systems Resources.** A key step in capability restoration is to **inventory systems resources** to help identify surreptitious adversary implants.

e. **Post-Attack Analysis.** Post-attack analysis provides information about **vulnerabilities exploited** and leads to **security improvements**. Audit trails such as automated recording of specific attack techniques during the incident can provide information required for analysis.

6. IO Attack or Potential Attack Response

IO attack detection or **validation of a potential attack** through analytical results of the I&W process trigger IO response. **Timely identification of actors and their intent** is the cornerstone of effective and properly focused response, thereby linking the analytic results of the I&W process to appropriate decision makers. This information should be disseminated by the JFC in a timely manner (See Figure III-8).

a. IO response involves **identifying actors and their intent** and **establishing cause and complicity** and also may involve appropriate action(s) against perpetrators. The effectiveness of the IO response is dependent upon **efficient integration of IO attack or potential attack detection and analysis capabilities**. IO response contributes to defensive IO by countering threats and enhancing deterrence.

b. Elements of the IO response may include **national-strategic decisions to apply flexible deterrent options**, either stand-alone or parallel. Possible response options include, but are not limited to, law enforcement, diplomatic actions, economic sanctions, and/or military force.

- **Law Enforcement.** Military and local law enforcement can contribute to information assurance by investigating information system incidents and intrusions and **apprehending criminals**. This may deter other criminals or adversaries. Law enforcement also provides **investigative resources** and **maintains records on incidents** which may assist analysts in defining vulnerabilities.

- **Diplomatic Actions.** Diplomatic actions can provide a powerful deterrent without resorting to lethal force. Diplomatic actions can be taken at **low**

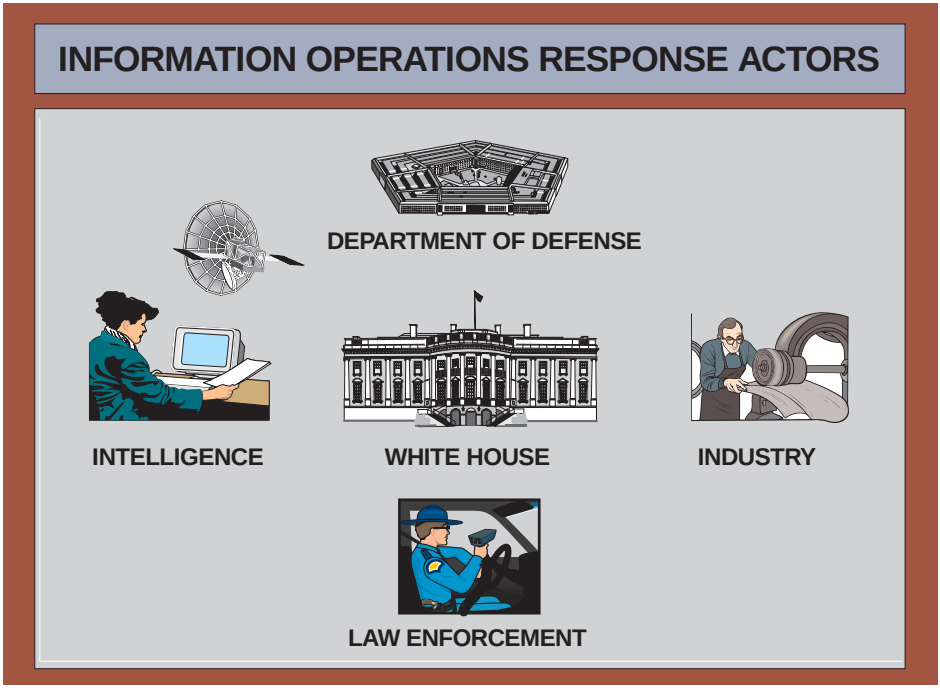


Figure III-8. Information Operations Response Actors

cost, are **scaleable**, and are **easily changed**. Additionally, diplomatic actions can be taken by individual states or as a group.

- **Economic Sanctions.** Economic sanctions offer another alternative to military force. **Economic sanctions may weaken an adversary's position**, thereby rendering him/her more susceptible to other response options. Economic sanctions have a number of weaknesses, however, including enforcement, which often relies on military force.

- **Military Force.** Military force includes a range of lethal and/or nonlethal responses that may **eliminate the threat directly** or **interrupt the means or systems that an adversary uses** to conduct IO .

"Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing."

Frederick the Great quoted in Foertsch, The Art of Modern War, 26 June 1996

Intentionally Blank

CHAPTER IV
INFORMATION OPERATIONS ORGANIZATION

"Organization is the vehicle of force, and force is threefold in nature; it is mental, moral, and physical."

Major General J.F.C. Fuller,
The Foundation of the Science of War, 1926

1. General

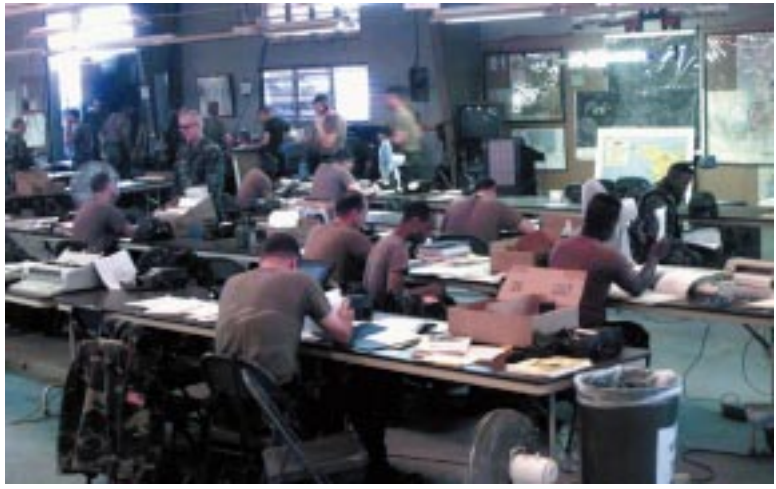
A fully functional IO cell is paramount to successful IO. The JFC's staff, which includes the IO cell, develops and promulgates guidance/plans for IO that are passed to the components and supporting organizations and agencies for detailed mission planning and decentralized execution. The IO cell integrates the broad range of potential IO actions and activities that help contribute to the JFC's desired end state in an AOR or JOA.

a. The **organizational structure** to plan and coordinate IO should be **sufficiently flexible** to accommodate a variety of planning and operational circumstances. This chapter focuses on organization for planning, coordinating, and executing IO.

b. **IO should be an integral part of all joint military operations.** This requires extensive planning and coordination among many elements of the joint headquarters, component staffs, and other USG departments and agencies to ensure IO are fully integrated with other portions of operation and campaign plans.

c. **Organizing to plan and coordinate IO is the JFC's responsibility.** Since JFCs are supported by staffs with diverse structure, scope of responsibilities, and supporting infrastructure, the commanders should tailor their organizations according to unique mission requirements.

d. The principal staffs that may be involved in IO planning are the **combatant command**, **subordinate joint force**



Information operational planning goes on at all staff levels

command(s), and **component staffs**. The circumstances in which these staffs conduct IO may affect the optimal organization.

- **The combatant command staffs**, supported by NSA and other Defense and intelligence agencies and Department of State representatives, **can call on the expertise of personnel assigned to their component commands** to assist in the planning process. These staffs use the planning process specified by the **Joint Operation Planning and Execution System** (JOPES) to carry out planning responsibilities. During crisis or other short-notice operations, the JOPES process is entered at the phase dictated by circumstances. The command which is designated the "supported command" will receive guidance and support from the NCA and can call on the expertise and technical support of all other commands designated "supporting commands."

- **A subordinate joint force** (normally a JTF) **may be designated to plan and/or execute IO on short notice**. With the exception of a few "standing" JTF staffs, these JTFs do not have the support of a permanent infrastructure. A JTF may be required to plan and/or execute IO immediately upon arrival in the operational area, while conducting forward presence operations, or after a short notice deployment while the infrastructure to support the staff is being developed.

- The IO cell, in coordination with other elements of the joint force staff, **develops and promulgates campaign or operation IO guidance for plans** that is passed down to the components or subordinate JTFs for decentralized execution.

- A component may be required to plan and execute IO **on short notice**, **immediately upon arrival** in an operational area after a short-notice deployment, or **while conducting forward presence operations**.

e. The IO cell is formed from **select representatives from each staff element, component, and supporting agencies** responsible for integrating capabilities and related activities. **This cell merges capabilities and related activities into a synergistic plan.** The cell coordinates staff elements and/or components represented in the IO cell to facilitate the detailed support necessary to plan and coordinate IO. Figure IV-1 provides an overview of a **typical joint IO cell**. The actual composition or members of the IO cell may vary based on the overall mission of the joint force, the role of IO in accomplishing the JFC's objectives, and the adversary's or potential adversary's capability to conduct IO. **The existing C2W cell should be reconfigured to function as the IO cell.** This provides the JFC with the capability to integrate, coordinate, and deconflict the full spectrum of IO.

2. Joint Force IO Organization

a. **JFC.** The JFC should **provide guidance** for planning and conducting IO and **assign responsibility** for the employment of IO resources in joint operations. In multinational operations, the US JFC may be responsible for coordinating the integration of US joint IO and multinational IO assets, strategy, and planning.

b. **Joint Staff Operations Officer.** The JFC normally will **assign responsibility for IO to a member of the joint staff**, usually the **Operations officer (J-3)**. When authorized, the J-3 will have primary staff responsibility for planning, coordinating, and integrating joint force IO.

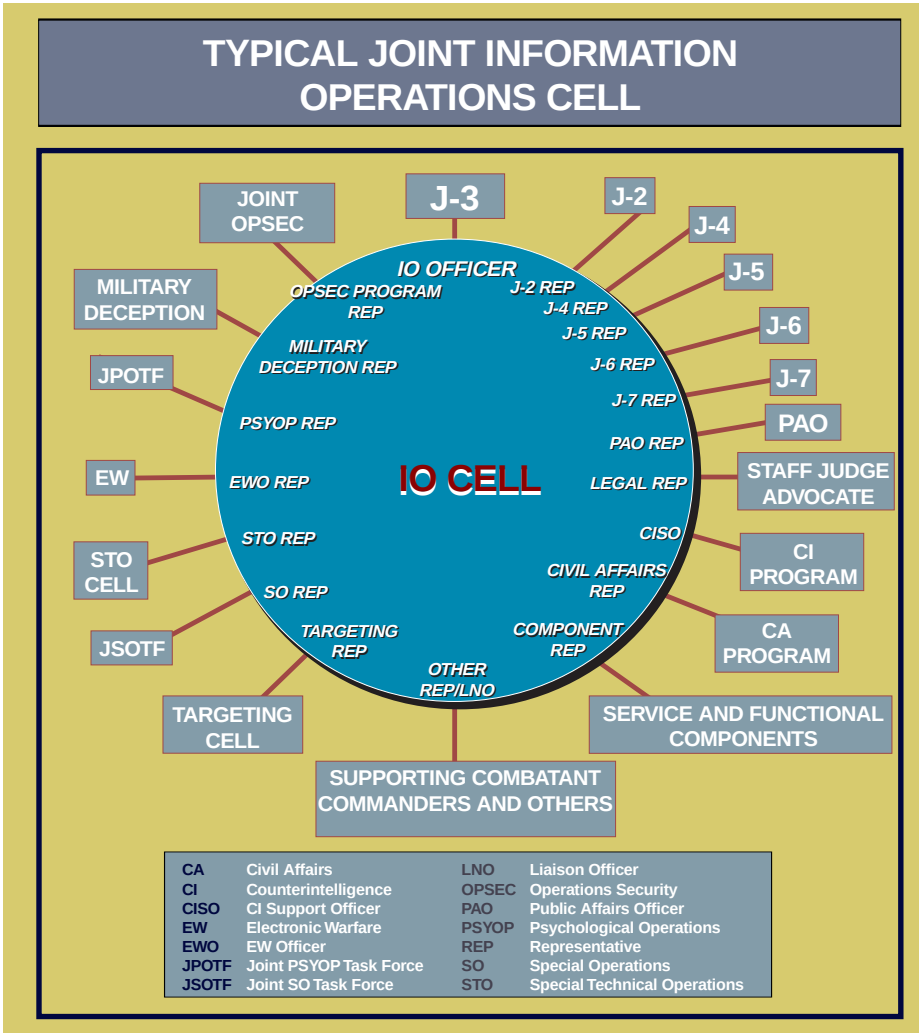


Figure IV-1. Typical Joint Information Operations Cell

c. **Organization**

- **IO Officer.** To assist the J-3 in exercising joint IO responsibilities, **the J-3 normally will designate an IO officer**. The primary function of the IO officer is to supervise the IO cell to ensure capabilities and activities are planned, coordinated, and integrated within the joint force staff and with higher echelon, adjacent, subordinate, and multinational staffs. **The IO officer will ensure IO is implemented per the JFC's guidance.** This may entail representing IO concerns at critical planning meetings, leading the IO cell, and/or directly facilitating coordination between the components or staff organizations responsible for planning and execution of IO. **The IO officer serves as JTCB** (or functional equivalent) **IO cell representative**. The IO officer is the central point of contact for IO and can coordinate all IO functional areas. The IO officer, or his/her designated representative, will

ensure **deconfliction** and **unity of effort** for information activities within an AOR/JOA. The IO officer normally ensures the functions shown in Figure IV-2 are performed.

•• **IO Cell Methods.** The procedures used by the IO cell to carry out assigned responsibilities should be **determined by the J-3 or IO officer**. During the **planning phases** of an operation, IO planners should facilitate the planning efforts between various staffs, organizations, and parts of the JFC staff responsible for planning elements of IO. During the **execution phase** of an operation, IO planners should be available to the joint operations center (JOC) or its equivalent to assist in deconfliction, support, or adjustment of IO efforts as necessary. If IO manning permits and the J-3 or IO officer designates, **IO personnel may be part of the JOC watch team** or stand a separate watch during the execution phase of an operation. IO personnel should have the **communications connectivity**, either through the JOC or separately, to effectively coordinate changing IO requirements during the execution phase. Due to the sensitive nature of some aspects of IO, all members of the IO cell should have appropriate security clearance and access necessary to fulfill their IO responsibilities.

•• **Planning Organizations of IO Representatives.** There are **planning**

INFORMATION OPERATIONS OFFICER FUNCTIONS

- **Coordinating the overall IO effort for the JFC.**
- **Coordinating IO issues within the joint staff and counterpart IO planners on the component staffs.**
- **Coordinating IO defensive and offensive concepts to support the JFC concept of operations.**
- **Establishing IO priorities to accomplish planned objectives.**
- **Determining the availability of IO resources to carry out IO plans.**
- **Recommending tasking to the J-3 for joint organizations, staff, and elements (e.g., electronic warfare planners, military deception planners, etc.) that plan and supervise the various capabilities and related activities to be utilized. Consolidated J-3 tasking ensures efficiency of effort in planning and executing integrated IO.**
- **Serving as the primary "advocate" for IO targets nominated for attack throughout the target nomination and review process established by the JFC.**
- **Coordinating the planning and execution of IO between the joint organizations (including components) responsible for each element of IO.**
- **Coordinating intelligence and assessment support to IO.**
- **Coordinating IO inputs from joint centers and agencies.**
- **Coordinating liaison with the Joint Command and Control Warfare Center, Joint Warfare Analysis Center, and other joint centers.**

Figure IV-2. Information Operations Officer Functions

organizations (e.g., joint psychological operations task force (JPOTF) and other planning organizations) **for the various representatives of the IO cell** which also have planning processes. The organizational relationships between the joint IO cell and these organizations are per JFC guidance. **These supporting organizations provide guidance** on the employment of their respective capabilities and activities both to the Service and functional components and to JFCs that have operational control of the forces. **The size, structure, and planning methods used by these planning organizations vary widely.** The specific duties and responsibilities of representatives from these supporting organizations should be established between the IO officer and the senior representative of each supporting organization. **Authorized staffing levels**, **mission**, and **location of JFC staff vis-à-vis each element-level organization** are among the considerations that should be taken into account in determining how element-level organizations are "represented" in the cell.

- **J-2 Representative.** Coordinates **collection requirements** and **analytical support** for compartmented and non-compartmented IO. May serve as liaison in the IO cell for Central Intelligence Agency, DIA, or NSA.

- **Logistics (J-4) Representative.** Coordinates and integrates **IO logistics considerations** into the deliberate planning process. Provides logistics policy guidance as appropriate.

- **Plans (J-5) Representative.** Integrates IO into the deliberate planning process. Provides **policy advice** as appropriate.

- **C4 (J-6) Representative.** Facilitates **IA coordination** between information system planners and managers and members of the IO cells. Coordinates with the J-3 to **minimize offensive IO operations impact** on own force C2. Principal liaison with the joint communications control center (JCCC). **Coordinates information system support** to the IO cell. May serve as the Joint COMSEC Monitoring Activity (JCMA) point of entry into the staff.

- **J-7 Representative.** Serves as primary **integrator of IO into exercises and M&S**, especially at the JTF level. Ensures resulting lessons learned are incorporated into the **Joint Universal Lessons Learned System**, as appropriate.

- **PSYOP Representative.** Integrates, coordinates, deconflicts, and synchronizes the use of **PSYOP,** to include multinational information activities, within a JFC's AOR or JOA that may support IO. Serves as entry point for liaison from JPOTF and the in-theater multinational PSYOP cells, as appropriate.

- **EW Representative.** Coordinates **EW activities**. Serves as **Joint Spectrum Center (JSC) liaison officer**. Coordinates closely with J-6 planner to deconflict friendly IO on the communications spectrum.

- **OPSEC Representative.** Coordinates combatant command or subordinate **joint force command OPSEC activities**. Works closely with J-6 planner for JCMA liaison.

- **Military Deception Representative.** Coordinates combatant command or subordinate joint force command **military deception planning**.

- **Special Technical Operations (STO).** The Joint Staff, combatant commands,

Service IO centers, and intelligence agencies all have STO organizations. They communicate through the Planning and Decision Aid System. The STO representative normally **coordinates Joint Warfare Analysis Center (JWAC) support and may coordinate JSC support**. The STO planner should be an integral member of the IO cell to ensure STO planning is fully integrated and coordinated.

- **Counterintelligence Support Representative.** Coordinates **IO inputs to CI activities** which have significant roles in both offensive and defensive IO.

- **Public Affairs Representative.** Coordinates **and deconflicts PA activities with planned IO**.

- **Legal/Staff Judge Advocate Representative.** Advises planners to **ensure IO comply with domestic and international law** and assists with interagency coordination and negotiation.

- **Civil Affairs Representative.** Ensures **consistency of CA activities** within the JFC's AOR or JOA that may support IO.

- **Special Operations Representative.** Coordinates **use of SOF** within a JFC's AOR or JOA in support of IO.

- **Targeting Representative.** Represents the **targeting cell(s)** and **coordinates IO targeting** with the JTCB, if designated.

- **Other Representatives and Liaison Officers.** Figure IV-1 is intended as a guide in determining **which members of a joint staff should coordinate with IO planners**. The JFC should tailor the composition of the cell as necessary to accomplish the mission. Other potential representatives include the following.

  •• **US Space Command and Operational Support Office Liaisons.** When available, may support the IO cell since space systems have broad applicability to the support of intelligence collection and information dissemination.

  •• **DISA.** Provides IA advice and guidance on matters pertaining to the DII and the Defense Communications System.

  •• **Information Operations Technology Center.** Provides technical support in the development, coordination, and deconfliction of certain aspects of IO planning.

  •• **NSA.** Provides INFOSEC and OPSEC products, tools, services, and vulnerability analyses.

  •• See Appendix A, "Supplemental Information Operations Guidance" (published separately), for additional organization guidance and responsibilities.

d. **Role of Functional and Service Component Representatives in IO.** Functional and Service component commanders should organize their staffs to plan and conduct IO. An **IO point of contact** or **IO officer** should be designated. This officer or an assistant will interface with the joint force IO cell to provide component expertise and act as a liaison for IO matters between the joint force and the component. These representatives also **may serve as members of one or more of the supporting organizations of IO** (e.g., the STO cell). Service and functional components requesting specific IO support from sources internal or external to the JFC normally should request such support through the respective joint force component headquarters to the JFC IO cell. Service IO organizations (e.g., Air Force Information Warfare Center, Land Information Warfare Activity, Fleet

Information Warfare Center) also may provide support to the IO cell through the appropriate Service component commanders.

e. **Role of Subordinate JTFs.** Subordinate JTFs normally share the same type of relationship with the parent joint force IO cell as the Service and functional components. **Subordinate JTFs 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 JTF.

f. **Role of Non-DOD US Government Agencies/Representatives of Multinational Forces and their Governments.** Non-DOD USG departments and agencies may have a role in the planning and accomplishment of IO. JFCs and their IO officers should ensure non-DOD US departments and agencies that have ongoing programs and interests in the AOR or JOA are **consulted in the development of IO plans**. The supporting non-DOD USG agencies should be **considered as part of the IO plan when appropriate**. Likewise, the potential contributions and concerns of multinational forces and their governments should be considered when appropriate.

"In war it is not always possible to have everything go exactly as one likes. In working with allies it sometimes happens that they develop opinions of their own."

Sir Winston Churchill,
The Hinge of Fate, 1950

3. Relationship with Joint Activities

a. **General.** As discussed above, **IO planners use other joint organizations to plan and integrate joint IO**. Support from these organizations includes, but is not limited to, personnel augmentation from JC2WC, JWAC, Joint Program Office for Special Technology Countermeasures (JPO-STC), JSC, and JCMA. Additionally, through the various organizations that plan and direct IO capabilities and elements of IO, **the IO planners have access to the Service or functional component expertise** necessary to plan the employment or protection of Service component systems or units.

b. **JC2WC.** The JC2WC may provide **direct support to the JTF through the JTF IO cell**. Normally this assistance is requested through the supported combatant commander, or directly from the JC2WC when such a direct relationship is authorized.

c. **JWAC.** The JWAC assists the Chairman of the Joint Chiefs of Staff and the combatant commanders in their preparation and analysis of joint operation plans and the Service Chiefs' analysis of weapon effectiveness. The JWAC provides **analysis of engineering and scientific data and integrates operational analysis with intelligence**. The JWAC normally will support a JTF through the supported combatant commander.

d. **JPO-STC.** The JPO-STC provides the combatant commanders, Military Services, and DOD mission planners with the **ability to assess their infrastructure dependencies and the potential impact on military operations** resulting from disruptions to key infrastructure components. Specific infrastructures addressed include electric power, natural gas, liquid petroleum, transportation, and telecommunications (Public Switched Network). JPO-STC also conducts **technical assessments of emerging special technologies** to determine their potential impacts to military and civilian systems and proposes countermeasure solutions and/or response options, as warranted.

e. **JSC.** The JSC can provide the following direct support to the JFC through the JFC IO cell.

- **Locational and technical characteristics** about friendly force C2 systems.

- **Assistance in development of the JFC joint restricted frequency list** (JRFL) for deconfliction purposes. The JSC may deploy an augmentation team trained to prepare JRFLs or provide training and assistance in how to prepare a JRFL.

- **Assistance in the resolution of operational interference and jamming incidents.** The JSC may deploy teams capable of quickly locating and identifying interference sources and recommending technical and operational fixes to resolve identified interference sources.

- **Data** about foreign C4 frequency and location data.

- **Unclassified C4 area studies** about the regional C4 infrastructure, to include physical and cultural characteristics, overview of telecommunications systems, and electromagnetic frequencies registered for use within the geographic boundaries of each country in the region.

f. **JCMA**

- Provides **INFOSEC monitoring and analysis support**.

- Provides a **joint COMSEC monitoring and analysis team** to provide direct, deployable joint COMSEC monitoring support. If tasked, the JCMA may manage all INFOSEC monitoring.

- Conducts **cryptographic or plain language system monitoring**.

- Provides **timely, tailored reporting** to supported commanders, to include near real time reporting of inadvertent disclosure of friendly critical information identified in the OPSEC process.

g. **Joint Communications Support Element (JCSE).** JTFs normally receive **tactical communications support**, to include augmentation by a wide array of tactical and commercial communications equipment **from the JCSE**.

h. **JCCC.** JFCs normally establish a JCCC to **support top level network control and management** within the AOR or JOA. JCCCs play a vital role in IO, particularly in the IA process, where they provide **J-6 connectivity** throughout the chain of command.

- **Combatant Command.** If established by the combatant command J-6, **the JCCC provides a conduit for secure interoperability issues** above and below the combatant command level. The JCCC can support the combatant command IO cell by **coordinating with the J-6** to integrate various disciplines and capabilities associated with protecting and defending information and information systems.

- **JTF.** When established, **the JTF JCCC provides the JTF IO cell with support** similar to that provided by the combatant command JCCC (when established), to include serving as a conduit throughout the chain of command for secure interoperability and deconfliction issues.

4. JTF IO Cell Relationships with Supporting DOD Agencies

a. **NSA.** If assigned an NSA representative, the JTF IO cell may receive direct support for the following.

- **INFOSEC technology, products, and services.**

- **Vulnerability and threat analyses** to support information assurance and the defense of US and friendly information systems.

- **Consultation and guidance** for use in determining exploitation risk for telecommunications systems.

- Assistance with **supporting and deconflicting national IO efforts** with combatant command and JTF IO efforts.

- Assistance in determining **release of COMSEC materials** to allies or coalition partners.

- **Other assistance** as described in Appendix A, "Supplemental Information Operations Guidance," (published separately).

b. **DIA.** A DIA representative to the JTF IO cell provides the following.

- **Precise and timely intelligence** for IO target selection and post-strike analysis.

- **Direct intelligence assistance** in the planning and execution of defensive IO.

- Assistance in identifying **friendly vulnerabilities** and the most **probable friendly targets** within the adversary's or potential adversary's capabilities and concept of operations.

- Assistance in developing **all-source intelligence gain/loss assessment** of IO targets.

c. **DISA.** When assigned a DISA representative, the following support will be provided to the JTF IO cell.

- **Coordination with DIA, NSA, and the Services** to ensure sufficient data base support for planning, analysis, and execution of IO.

- Assistance in **disseminating warnings of CNA**.

- Assistance in **establishing a security architecture and standards** for protecting and defending the DII within the JOA.

- Development of an **information system incident program** and a **security incident response** capability for protecting and defending the DII within the JOA.

- Assessment of the **vulnerabilities of information and information systems** and development within available capabilities of procedures to mitigate assessed vulnerabilities and threat effects.

- Development of **INFOSEC education, training, and awareness program guidelines**, including minimum training standards, for use by the JTF headquarters, components, and subordinate JTFs.

"The primary object of organization is to shield people from unexpected calls upon their powers of adaptability, judgment, and decisions."

General Sir Ian Hamilton,
Soul and Body of an Army, 1921

Intentionally Blank

CHAPTER V
INFORMATION OPERATIONS PLANNING

"War plans cover every aspect of a war, and weave them all into a single operation that must have a single, ultimate objective in which all particular aims are reconciled."

Major General Carl von Clausewitz
On War, viii, 1832, tr. Howard and Paret

1. IO Planning Methodology

a. **General**

- IO planning is accomplished in both the **deliberate and crisis action planning processes** and is incorporated in the JFC's overall operations planning.

- IO planning must be **broad-based** and encompass employment of **all available IO resources** — joint, Service, interagency, and multinational.

- IO planning must begin at the **earliest stage** of a JFC's campaign or operation planning. Ideally, peacetime IO planning within a combatant commander's AOR will provide a basis for subsequent IO in war and MOOTW in that AOR.

- IO planning must **analyze the risk** of compromise, adversary reprisal, collateral damage, escalation of hostilities, and uncoordinated or inadvertent counteraction of IO activities by the various joint, Service, and/or interagency IO capability providers that may be released to the combatant commander for employment.

b. **IO Planning Fundamentals.** Planning for employment of IO begins with articulating and understanding the JFC's mission, concept of operations, **objectives**, and **intent**. A joint campaign is the synchronization of air, land, sea, space, and special operations (as well as interagency and multinational operations) in harmony with diplomatic, economic, and IO efforts to attain national and multinational objectives. The same **fundamentals of campaign planning** shown in Figure V-1 apply to the IO portion of a plan. Some of these fundamentals are particularly important in planning and execution of IO.

- **The synchronization and integration of the IO requires clear national strategic guidance.** The National Security Strategy and National Military Strategy, shaped by and oriented on national security policies, must provide strategic direction to combatant commanders. This direction is required **to ensure JFC IO planning supports national objectives**. Combatant commanders, in turn, provide guidance and direction through their combatant command strategies and plans for the employment of military forces, in conjunction with interagency and multinational forces, for the conduct of military operations. **These strategies should support combatant commander objectives** across the range of military operations. Combatant commanders and subordinate JFCs must consider the **strategic environment** during the estimate and planning process in order to determine potential constraints and opportunities. **JFCs must provide components and subordinate joint forces critical planning guidance** such as actions that must be accomplished (constraints), actions that must be avoided (restrictions), and planning

FUNDAMENTALS OF CAMPAIGN PLANS

- Provide broad strategic concepts of operations and sustainment for achieving multinational, national, and theater strategic objectives.
- Provide an orderly schedule of decisions.
- Achieve unity of effort with air, land, sea, space, and special operations forces, in conjunction with interagency, nongovernmental, or private voluntary organizations or United Nations or other multinational forces, as required.
- Incorporate the combatant commander's strategic intent and operational focus.
- Identify any special forces or capabilities the enemy has in the area.
- Identify enemy strategic and operational centers of gravity and provide guidance for defeating them.
- Identify friendly strategic and operational centers of gravity and provide guidance to subordinates for protecting them.
- Sequence a series of related major joint operations conducted simultaneously in depth.
- Establish the organization of subordinate forces and designate command relationships.
- Serve as the basis for subordinate planning and clearly define what constitutes success, including conflict termination objectives and potential posthostilities activities.
- Provide strategic direction, operational focus, and major tasks, objectives, and concepts to subordinates.
- Provide direction for the employment of nuclear weapons as required and authorized by the National Command Authorities.

Figure V-1. Fundamentals of Campaign Plans

factors that have not been confirmed but must be considered true in order to complete planning requirements (assumptions). This guidance will establish the "boundaries" for IO planning, identify target limitations based on policy, and help reduce the uncertainty associated with IO planning. These constraints often limit the JFC's freedom of action and influence the timing and form of the campaign.

- **IO planning requires an orderly schedule of decisions.** Many IO will require long-term development of intelligence and preparation of the battlespace for use of capabilities. The use of IO in peacetime as a principal means to achieve JFC objectives and preclude other conflict requires an ability to integrate IO capabilities into a coherent strategy.

- **Establishing the organization of subordinate forces and designating command relationships** also is very important in developing and executing IO. Establishing these relationships is

the basis for achieving **unity of command and effort** among air, land, sea, space, and special operations forces. This also establishes **interagency agreement** on the synchronization, coordination, and deconfliction process for IO planning and execution.

- During planning for IO, the planners will **identify adversary vulnerabilities**, **devise required tasks and sub-tasks**, and **identify access (opportunities)** and the means to exploit these vulnerabilities to achieve the JFC's objectives. The means or capabilities used by the JFC will vary from organic non-compartmented capabilities to national level capabilities. This requires the planners to **identify Service, joint, and interagency IO capabilities available to the JFC for planning purposes**, thereby providing a "toolbox" for the JFC to use in developing an IO plan and facilitating an effective capability-to-target match. As part of the planning process, designation of release and execution authority is required. **Designation of approval authority** for some IO may be 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 defined as the authority to conduct IO at a designated time and/or place. Normally, there is one execution authority, which is the supported JFC.

"Know the enemy and know yourself; in a hundred battles, you will never be in peril."

Sun Tzu, The Art of War

- The **identification of the adversary strategic and operational centers of gravity** and guidance for defeating them is **fundamental to IO planning** in support of the JFC's campaign planning. IPB for IO differ from traditional requirements in that they may need greater lead time and may have expanded collection requirements. Figure V-2 shows a means to template IO planning and assessments. See Appendix A, "Supplemental Information Operations Guidance" (published separately), for additional guidance.

- Identifying and providing guidance on **protecting the friendly centers of gravity and critical information infrastructures** at the JFC operational level and at the strategic level are crucial. Identifying friendly information priorities requires **close coordination and cooperation between DOD, other USG departments and agencies, and industry**. Protection of the information infrastructure requires collaborative efforts to implement protective measures commensurate with the value of the information or information systems protected. Adherence to a **common level of protection** requires determining the scope of what needs to be protected and the standards for how much protection is needed.

c. **IO Cell**

- At the combatant and subordinate joint force command levels, the **IO cell is the focal point for IO planning**, to include coordination, integration, and deconfliction.

- The IO cell should **exchange information with cell members** about plans in development. The IO cell should focus on **integration** and **deconfliction** of capabilities to accomplish mission objectives.

- **The IO cell should be represented in all joint force planning activities.** The relationship of the IO cell to other

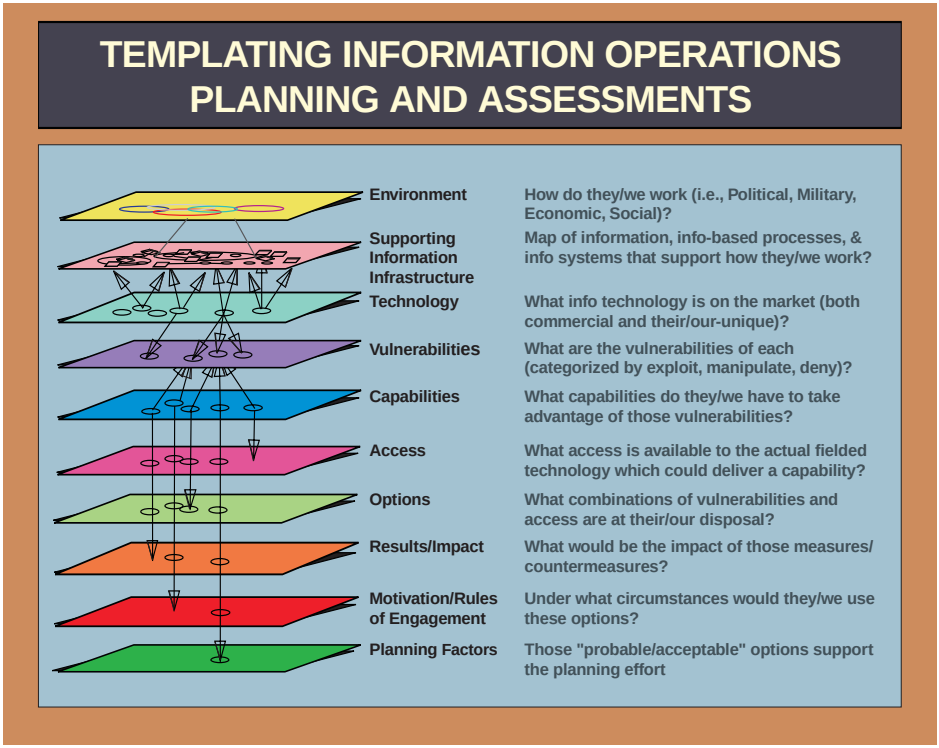


Figure V-2. Templating Information Operations Planning and Assessments

planning activities is provided in the coordination paragraph below.

2. IO Planning Coordination

a. **General.** IO coordination is continuous across **all phases of an operation** and the **range of military operations** and **at every level of war**. IO planning must account for postconflict activities which require transition of IO to foreign military or USG nonmilitary agencies or organizations.

b. **Joint Planning Group. JFCs normally establish a joint planning group (JPG)**, particularly at the JTF level. If a JPG is established, **the IO cell must be represented** in the JPG. Early and continuous exchange of information and close coordination of planning activities between the JPG and the IO cell is essential to successful integration of IO planning in the overall JOPES process.

c. **JTCB.** IO cell representation to the JTCB, if designated, can provide **the conduit for ensuring effective IO coordination** and normally also will provide a means to coordinate joint force capabilities with the application of IO and other conventional operations.

3. IO Integration and Deconfliction

a. **IO Integration.** IO require **early integration between components, groups, organizations, and agencies** involved in planning and executing IO actions and activities. Just as IO execution must be integrated with all other facets of joint operations, so must IO planning be integrated.

Providing a forum to coordinate, integrate, and deconflict IO within the joint force is the critical function of the IO cell.

- IO integration should be accomplished at the **lowest practicable level**. As a result of mission-type orders issued to components or subordinate JTFs, IO execution often is decentralized.

- The IO cell should provide the **overall integration strategy** for IO and ensure capabilities are integrated.

  •• The IO cell normally has the **assigned personnel, communications linkages, and connectivity** with J-6 and defensive IO providers to effectively integrate defensive IO planning.

  •• The IO cell also **maintains connectivity with other government organizations and activities** such as NSA, DIA, and DISA, who have a distinct role in defensive IO.

- **Compartmented Capabilities**

  •• Members of the IO cell possessing the proper security clearance and access **integrate compartmented capabilities into plans**. Normally, the cell is the appropriate entity to conduct this integration. In addition, the IO cell has the **connectivity to higher authority for plan approval** normally associated with compartmented operations.

  •• **Close coordination between the IO cell and the joint force STO cell** is essential to this integration effort. JFCs should use the guidance in Annex S of Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance," to facilitate this process. Additional considerations are addressed in Appendix A, "Supplemental Information Operations Guidance," (published separately).

b. **IO Deconfliction. IO deconfliction may be required at several levels**, i.e., within, above, and below the joint force, and at several levels of war. In addition, **offensive and defensive IO may need to be deconflicted at the same level**. As with integration, deconfliction of IO should begin at the earliest possible stage of IO planning.

- IO deconfliction should be a **continuous process** which allows for **flexible phasing** of IO employment options. The likelihood of simultaneous IO at all levels of war and command is quite high. Additionally, the relatively large number of potential capability providers in the same AOR or JOA, particularly when IO are a main element of a JFC's operations, makes **early identification of IO deconfliction issues essential**.

- **The IO cell provides the best entity for coordinating and overseeing IO deconfliction.** The IO cell has connectivity with all IO providers within the joint force. In addition, the IO cell has connectivity with IO cells higher and lower in the chain of command. Finally, the IO cell works with and has input to defensive IO within the joint force, thereby providing the IO cell with the best overall view for ensuring IO deconfliction.

- See Appendix A, "Supplemental Information Operations Guidance" (published separately), for compartmented IO deconfliction considerations.

4. JOPES Guidance for IO Planning

a. **General. IO plans should be developed in support of the JFC's overall operational planning** in either the deliberate or crisis action planning processes. To accomplish this, **IO planning should occur simultaneously with operation planning**. CJCSM 3122.03, "Joint Operation Planning and Execution System Volume II, Planning Formats and Guidance," is the operational planner's guide to developing OPLANs through the deliberate planning process.

- **IO in the Deliberate Planning Process.** Figure V-3 provides a **general guide to IO planning** as an integrated part of the JOPES deliberate planning process at the combatant command level. The figure may be adapted for similar IO planning guidance at the subordinate joint force and component levels as required. When IO planning is being conducted below the combatant command level, **the IO cell should keep the IO cell at the next higher level of command fully apprised** of all IO deliberate planning activities which may require synchronization, coordination, or deconfliction.

- **IO in the Crisis Action Planning Process.** In contrast to deliberate planning, crisis action planning normally takes place in a compressed time period. In crisis action planning, coordination of the IO plan is even more crucial than in deliberate planning. Figure V-4 provides a general guide to IO planning as an integrated part of the JOPES crisis action planning at the combatant command level. As with Figure V-3, Figure V-4 may be adapted as required for similar IO planning guidance at the subordinate joint force and component levels.

b. **IO JOPES Guidance.** The final IO JOPES planning product in both deliberate and crisis action planning is an approved **Appendix 3 to Annex C**. This appendix also contains the overall concept for both offensive and defensive IO with respect to the plan or OPORD in which it appears. For **deliberate planning**, this appendix will be included in an OPLAN, OPLAN in concept format (CONPLAN) (with or without time-phased force and deployment data), or a functional plan. For **crisis action planning**, this appendix will be included in a campaign plan or an OPORD. Specific guidance on the preparation of this appendix is in Appendix B, "JOPES Information Operations Guidance."

c. **Defensive IO JOPES Guidance.** The final defensive IO JOPES planning product in both deliberate and crisis action planning is an approved **Appendix 2 to Annex K**. As with the JOPES appendix for offensive IO, this appendix will be included in the various plans and OPORDs produced in JOPES deliberate and crisis action planning. Specific guidance on the preparation of this appendix is in Appendix C, "JOPES Defensive Information Operations Guidance."

"The stroke of genius that turns the fate of a battle? I don't believe in it. A battle is a complicated operation, that you prepare laboriously. If the enemy does this, you say to yourself I will do that. If such and such happens, these are the steps I shall take to meet it. You think out every possible development and decide on the way to deal with the situation created. One of these developments occurs; you put your plan in operation, and everyone says "What genius . . ." whereas the credit is really due to the labor of preparation."

Ferdinand Foch,
Interview, April 1919

INFORMATION OPERATIONS PLANNING RELATED TO DELIBERATE PLANNING

PLANNING PHASE	JOPES	IO CELL PLANNING ACTION	IO PLANNING OUTCOME
PHASE I	Initiation	Notify IO cell members of planning requirements.	N/A
PHASE II	Concept Development		
Step 1	Mission Analysis	IO cell identifies information requirements needed for mission planning.	Tasking to gather/obtain required information.
Step 2	Planning Guidance	IO cell assists in development of combatant commander's IO planning guidance to support overall operational planning guidance.	Combatant commander's planning guidance for IO.
Step 3	Staff Estimates	IO cell supports the development of intelligence, operations, and communications staff estimates.	IO portion of staff estimates.
Step 4	Commander's Estimate	IO cell assists in transforming staff estimates into the Commander's Estimate.	IO portion of Commander's Estimate.
Step 5	Combatant Commander's Concept	IO cell assists in the IO aspect of Combatant Commander's Concept as required.	IO portion of Combatant Commander's Concept.
Step 6	CJCS Concept Review	IO cell assists in the IO aspect of CJCS Concept Review as required.	IO portion of operational concept approved by CJCS.
PHASE III	Plan Development	IO cell develops the complete IO plan and the plans for each of the IO elements in coordination with appropriate staff sections, operational units, and supporting agencies.	Draft offensive and defensive IO appendices with element tabs.
PHASE IV	Plan Review	IO cell modifies/refines plan as necessary.	Approved offensive and defensive IO appendices.
PHASE V	Supporting Plans	Subordinate units and supporting agencies prepare their own IO plans. IO cell coordinates/assists subordinate and supporting IO plan as necessary. Ensure TPFDD supports IO plan.	Completed subordinate and supporting agencies' supporting plans. IO plan supported by TPFDD.

CJCS = Chairman of the Joint Chiefs of Staff
IO = Information Operations
TPFDD = Time-Phased Force and Deployment Data

Figure V-3. Information Operations Planning Related to Deliberate Planning

INFORMATION OPERATIONS PLANNING RELATED TO CRISIS ACTION PLANNING			
PLANNING PHASE	**JOPES**	**IO CELL PLANNING ACTION**	**IO PLANNING OUTCOME**
PHASE I	Situation Development	IO cell identifies planning information requirements as situation develops.	Tasking to gather/obtain required information.
PHASE II	Crisis Assessment	IO cell identifies information requirements needed for mission planning. IO cell assists in development of combatant commander's IO planning guidance to support overall operational planning guidance.	IO planning guidance. Initial liaison with units and agencies that may participate in or support IO operations.
PHASE III	Course of Action Development	IO cell supports the development of intelligence, operations, and communications staff estimates.	IO portion of staff estimates.
PHASE IV	Course of Action Selection	IO cell assists in transforming staff estimates into the Commander's Estimate. IO cell assists in the IO aspect of Combatant Commander's Concept as required.	IO portion of overall plan approved through CJCS.
PHASE V	Execution Planning	IO cell develops the complete IO plan and the plans for each of the IO elements in coordination with appropriate staff sections, operational units, and supporting agencies.	Approved offensive and defensive appendices with element tabs, completed supporting plans, and inclusion of IO requirements in TPFDD.
PHASE VI	Execution	IO cell monitors IO operations and adapts IO objectives to support changing operational directives.	IO objectives modified as necessary to support changing operational objectives.
CJCS = Chairman of the Joint Chiefs of Staff IO = Information Operations TPFDD = Time-Phased Force and Deployment Data			

Figure V-4. Information Operations Planning Related to Crisis Action Planning

CHAPTER VI
INFORMATION OPERATIONS IN TRAINING, EXERCISES, AND MODELING AND SIMULATION

"Sufficient training, including realistic exercises that simulate peacetime and wartime stresses, shall be conducted to ensure that commanders of US Armed Forces are well-informed about trade-offs among affecting, exploiting, and destroying adversary information systems, as well as the varying capabilities and vulnerabilities of DOD information systems."

DODD S-3600.1, Information Operations

1. Essential Elements in IO Training

a. **General**

- Effective employment of IO in joint operations depends on the ability to **organize and train in the manner the United States intends to employ military force**. The basic training task is to train those personnel and organizations responsible for planning and conducting IO on the concepts and doctrine found in this publication.

- JFCs should ensure that **key personnel responsible for planning and conducting IO receive joint training** in both offensive IO and defensive IO. This training should focus on the AOR or JOA where IO are likely to be conducted. In addition, this training should build upon ongoing **peacetime** IO activities within each combatant commander's AOR and transition to **crisis deterrence** or **conflict resolution**, as appropriate.

- The **Joint Professional Military Education system** should ensure officers understand the role IO play in joint operations, either as the main effort or as a supporting function.

- The Services are responsible for **individual and unit training** in offensive and defensive IO.

b. **Offensive IO Training**

- Offensive IO training should include **integration of all available and potentially available offensive capabilities to conduct IO**, to include multinational and other DOD and non-DOD offensive capabilities.

- Offensive IO training should consist of both **individual and organizational training** and should emphasize planning with all offensive capabilities.

- Offensive IO training should focus on the three possible aspects of offensive IO employment: **offensive IO as the main effort, offensive IO as a supporting effort, and offensive IO as a phase of the operation**.

c. **Defensive IO Training**

- Defensive IO training should include **integration of all available defensive capabilities**, to include commercial and other DOD and non-DOD defensive capabilities.

- Defensive IO training should include both **individual and organizational training** and should emphasize the protection and defense of information and information systems.

- Defensive IO training should build upon the **routine peacetime information and information systems protection procedures** used throughout the Department of Defense and other USG and commercial activities.

2. IO in Joint Exercises

a. **General**

- **All joint exercises should incorporate IO appropriate to the scope and duration of the exercise.** Only during joint exercises can the complexity of synchronization, coordination, and deconfliction of IO within the joint force and throughout the Department of Defense and other USG and commercial activities be made apparent to the planners and implementors of IO. When feasible, joint exercises should incorporate the challenges of coordinating IO activities with multinational forces, international organizations, and nongovernmental organizations (NGOs).

- Joint exercises may incorporate IO training in three ways: **stand-alone**, **supported**, and **supporting**.

  •• **Stand-Alone:** IO is the only strategy used to affect an adversary.

  •• **Supported:** IO is the main effort, supported by other joint operations as required.

  •• **Supporting:** IO is used as a force multiplier within a conventional campaign.

- Figure VI-1 contains fundamental IO joint exercise planning considerations.

FUNDAMENTAL INFORMATION OPERATIONS EXERCISE PLANNING CONSIDERATIONS

- **Develop concrete, attainable IO objectives.**
- **Provide for sufficient IO actions to support the objectives of the exercise.**
- **Create as realistic an IO exercise environment as possible.**
- **Assess and evaluate the employment of IO.**
- **Exercise both offensive and defensive IO using all the capabilities that are available and compatible with the exercise scenario.**
- **Exercise intelligence support to IO.**
- **Use appropriate security measures to protect IO tactics, techniques, and procedures.**
- **Evaluate the use of computer support products to plan and evaluate IO operations.**
- **Evaluate the use of simulations to fulfill some IO training objectives.**

Figure VI-1. Fundamental Information Operations Exercise Planning Considerations

Predator UAV supporting joint exercise

b. **Offensive IO**

- Offensive IO planning and execution in joint exercises should emphasize **offensive IO attack** and use of all capabilities normally available to the joint force conducting the exercise.

- Offensive capabilities in joint exercises should be provided **appropriate intelligence support**, particularly intelligence concerning the OPFOR. In addition, the OPFOR should be allowed realistic free play to provide an appropriate challenge to both friendly intelligence development and IO targeting efforts.

c. **Defensive IO**

- Defensive IO planning and execution in joint exercises should emphasize **protection and defense of information** and **information systems**. Defensive capabilities normally available to the joint force should be exercised.

- Defensive IO planning in joint exercises also should include **protective and defensive considerations** for other DOD, other USG, and commercial supporting communications infrastructures. Planning also should consider coordinating protective and defensive measures for multinational forces, international organizations, and NGOs.

- As in offensive IO play in joint exercises, **the OPFOR should be allowed realistic free play** to ensure defensive capabilities are stressed or exercised to the appropriate degree. **Exercise design should allow the C2 and other information deprivation chaos** that arises when ineffective defensive IO measures are planned and implemented, consistent with the overall training objectives of the exercise. This will allow joint force participants to test the methodology of dealing with IO attacks as well as work through defensive IO problems caused by effective adversary IO.

- **CNA Red Teaming.** CNA red teaming can be a key element for an OPFOR in an IO-related joint exercise. **CNA red teaming is an independent and threat-based effort using active and passive capabilities and activities.** Red teams

use formal, time-bounded tasking to expose and exploit friendly force vulnerabilities.

3. IO in Planning and Modeling and Simulation

a. **General. IO should be incorporated in all planning and M&S** at the earliest practicable stage of model development. Only in this fashion can IO M&S be integrated appropriately with M&S for the other warfare areas.

b. **IO in Planning Models**

- **Offensive IO.** Planning models should incorporate **offensive capabilities and principles to conduct IO**, to include offensive capabilities normally organic to US military forces and other DOD and non-DOD USG agencies and organizations. **Multinational offensive capabilities should be included** as they become known and available for planning purposes.

- **Defensive IO.** Planning models should include **potential defensive capabilities** from the US military, **other DOD and non-DOD USG sources**, international organizations, NGOs, and such **commercial defensive capabilities** as may reasonably be expected to be available for planning purposes. Potential multinational defensive capabilities also should be catalogued and included in planning models.

c. **IO in M& S**

- **Offensive IO. Offensive capabilities to conduct IO should be incorporated in M&S** to allow realistic free play between friendly joint forces and the OPFOR. Where possible and when practicable, offensive IO should be **tailored to fit the offensive capabilities of the participating friendly forces** and the likely OPFOR for the exercise AOR or JOA. In addition, multinational offensive capabilities likely to be made available for planning and operations in the region should be added to the model(s) to the extent possible.

- **Defensive IO.** Defensive capabilities organic to the exercising force and other DOD and non-DOD USG agencies and organizations likely to be available in the exercise AOR or JOA should be added to exercise model(s). **Commercial defensive capabilities** and **multinational, international organization, and NGO defensive resources** known to be available in the affected exercise region **should be added to the extent possible**. This will allow realistic M&S IO play between the joint force and its multinational partners and the OPFOR.

- **Assessment and Evaluation.** The model(s) used in IO M&S should provide a means to **assess and evaluate IO employment in both offensive and defensive IO** and **allow for unambiguous feedback** to exercise participants, both the friendly forces and the OPFOR. The evaluation and assessment also should provide a **means to control IO play** and **make adjustments** if supporting IO adversely affect or negate the other objectives of the exercise.

"In no other profession are the penalties for employing untrained personnel so appalling or so irrevocable as in the military."

General Douglas MacArthur, US Army Chief of Staff, 1933

APPENDIX A
SUPPLEMENTAL INFORMATION OPERATIONS GUIDANCE

This appendix is a classified supplement provided under separate cover. The classified Appendix expands on information contained in this publication.

Intentionally Blank

APPENDIX B
JOPES INFORMATION OPERATIONS GUIDANCE

Annex	A	JOPES IO (Military Deception) Guidance
	B	JOPES IO (Electronic Warfare) Guidance
	C	JOPES IO (Operations Security) Guidance
	D	JOPES IO (Psychological Operations) Guidance
	E	JOPES IO (Physical Destruction) Guidance
	F	JOPES IO (Public Affairs) Guidance
	G	JOPES IO (Civil Affairs) Guidance

JOPES INFORMATION OPERATIONS GUIDANCE

The guidance in this appendix relates to the development of Appendix 3 (Information Operations) to Annex C (Operations) of the OPLAN/CONPLAN/OPORD/campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **Enemy**

- What are the enemy situation, force disposition, intelligence capabilities, and possible COAs?
- Is there any specific information that bears directly on the planned IO?

b. **Friendly**

- What is the situation of friendly forces that may directly affect attainment of IO objectives?
- Are there any critical limitations and other planned IO?

c. **Assumptions**

- What are the assumptions concerning friendly, enemy, or third-party capabilities, limitations, or COAs?
- What conditions does the commander believe will exist when the plan becomes an order?

2. Mission

What is the IO mission (who, what, when, where, why)?

3. Execution

a. **Concept of Operations**

- How does the commander visualize the execution of IO from beginning to termination?
- How will IO support the commander's mission?
- What are the concepts for supervising and terminating IO?

b. **IO Tasks**

- What are the major tasks for military deception? See Annex A, "JOPES IO (Military Deception) Guidance," for further guidance.
- What are the major tasks for EW? See Annex B, "JOPES IO (Electronic Warfare) Guidance," for further guidance.
- What are the major tasks for OPSEC? See Annex C, "JOPES IO (Operations Security) Guidance," for further guidance.
- What are the major tasks for PSYOP? See Annex D, "JOPES IO (Psychological Operations) Guidance," for further guidance.
- What are the major tasks for physical destruction related to IO? See Annex E, "JOPES IO (Physical Destruction) Guidance," for further guidance.
- What are the major tasks for PA? See Annex F, "JOPES IO (Public Affairs) Guidance," for further guidance.

- What are the major tasks for CA? See Annex G, "JOPES IO (Civil Affairs) Guidance," for further guidance.

c. **Coordinating Instructions.** What, if any, are the mutual support issues relating to the elements of IO?

4. Administration and Logistics

a. What are the administrative requirements related to IO?

b. What are the logistics requirements related to IO?

5. Command and Control

a. What are the C2 instructions related to IO?

b. What is the command structure for IO?

c. Are there any special communications and reporting requirements for IO? If so, what are they?

Intentionally Blank

ANNEX A TO APPENDIX B
JOPES IO (MILITARY DECEPTION) GUIDANCE

The guidance in this annex relates to the development of Tab A (Military Deception) of Appendix 3 (Information Operations) to Annex C (Operations) of the OPLAN/CONPLAN/OPORD/campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **General.** What is the general overall situation concerning military deception?

b. **Enemy**

- **General Capabilities.** What are the enemy military capabilities relating directly to the planned deception?
- **Deception Targets.** What are the deception targets?
- **Target Biases and Predispositions.** What are the target biases and predispositions?
- **Probable Enemy COA.** What is the probable enemy COA? (Refer to Annex B (Intelligence) of the basic plan.)

c. **Friendly**

- What is the friendly forces situation?
- What, if any, are the critical limitations?
- What is the concept of friendly operations?

d. **Assumptions**

- What are the assumptions concerning friendly, enemy, or third-party capabilities, limitations, or COAs?
- What conditions does the commander believe will exist when the plan becomes an order.

2. Mission

a. **Operational Mission.** See paragraph 2 of the basic plan or order.

b. **Deception Mission**

- **Deception Goal.** What is the desired effect or end state the commander wishes to achieve?
- **Deception Objective(s).** What is the desired action or inaction by the adversary at the critical time and location?
- **Desired Enemy Perceptions.** What must the deception target believe for him/her to make the decision that will achieve the deception objective?
- **Deception Story.** What scenario will cause the deception target to adopt the desired perception? Consider one of the COAs discarded during plan preparation.

3. Execution

a. **Concept of the Operation**

- **General.** What is the framework for the operation? Include a brief description of the phases of the deception operation.

- **Other IO Capabilities**

  •• What other capabilities will be used to support the deception operation?

  •• What are the other plans and operations pertinent to the deception?

  •• What coordination and deconfliction is required?

- **Feedback and Monitoring**

  •• What type of feedback is expected, if any, and how will it be collected?

  •• What impact will the absence of feedback have on the plan?

- **Means.** By what means will the deception be implemented?

- **Tasks.** What are the execution and feedback taskings to organizations participating in the execution and monitoring of the deception?

- **Risks**

  •• Deception is successful. What is the likely adversary response? What will be the impact on friendly forces from adversary intelligence sharing?

  •• Deception fails. What is the impact if the deception target ignores the deception or fails in some way to take the actions intended?

  •• Deception is compromised to multinational partners or adversaries. What is the impact of such compromise on friendly forces and attainment of friendly objectives?

b. **Coordinating Instructions**

- What are the tasks or instructions listed in the preceding subparagraphs pertaining to two or more units?

- What is the tentative D-day and H-hour, if applicable, and any other information required to ensure coordinated action between two or more elements of the command?

4. Administration and Logistics

a. **Administration**

- **General.** What are the general procedures to be employed during planning, coordination, and implementation of deception activities?

- **Specific.** What, if any, are the special administrative measures required for the execution of the deception operation?

b. **Logistics.** What are the logistics requirements for the execution of the deception operation (transportation of special material, provision of printing equipment and materials)?

c. **Costs.** What are the applicable costs associated with the deception operation?

NOTE: Do not include those administrative, logistics, and medical actions or ploys that are an actual part of the deception operation.

5. Command, Control, and Communications

a. **Command Relationships**

- **Approval.** What is the approval authority for execution and termination?

- **Authority.** Who are the designated supported and supporting commanders and supporting agencies?

- **Oversight.** What are the oversight responsibilities, particularly for executions by non-organic units or organizations outside the chain of command?

- **Coordination**

  •• What are the in-theater coordination responsibilities and requirements related to deception executions and execution feedback?

  •• What are the out-of-theater coordination responsibilities and requirements related to deception executions and execution feedback?

b. **Communications**

- What are the communications means and procedures to be used by control personnel and participants in the deception operation?

- What are the communications reporting requirements to be used by control personnel and participants in the deception operation?

6. Security

a. **General.** What are the general security procedures to be employed during planning, coordination, and implementation of deception activities?

b. **Specific**

- What are the access restrictions and handling instructions to the deception appendix or plan?

- Who has authority to grant access to the deception appendix or plan?

- How will cover stories, codewords, and nicknames be used?

- How will planning and execution documents and access rosters be controlled and distributed?

NOTE: Additional exhibits to TAB A (Military Deception) of Appendix 3 (Information Operations) to Annex C (Operations) of the OPLAN/CONPLAN/OPORD/campaign plan/functional plan may be required as shown below. Detailed instructions for the preparation of these exhibits is in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

Exhibits:

1 — Task Organization

2 — Intelligence

3 — Operations

4 — Administration and Logistics

5 — Command Relationships

6 — Execution Schedule

7 — Distribution

Intentionally Blank

ANNEX B TO APPENDIX B
JOPES IO (ELECTRONIC WARFARE) GUIDANCE

The guidance in this annex relates to the development of Tab B (Electronic Warfare) of Appendix 3 (Information Operations) to Annex C (Operations) of the OPLAN/CONPLAN/OPORD/campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **Enemy Forces**

- What are the capabilities, limitations, and vulnerabilities of enemy communications, non-emitting, and EW systems?
- What is the enemy capability to interfere with accomplishment of the EW mission?

b. **Friendly Forces**

- What friendly EW facilities, resources, and organizations may affect EW planning by subordinate commanders?
- Who are the friendly foreign forces with which subordinate commanders may operate?

c. **Assumptions.** What are the assumptions concerning friendly or enemy capabilities and COAs that significantly influence the planning of EW operations?

2. Mission

What is the EW mission (who, what, when, where, why)?

3. Execution

a. **Concept of Operations**

- What is the role of EW in the commander's IO strategy?
- What is the scope of EW operations?
- What methods and resources will be employed? Include organic and non-organic capabilities.
- How will EW support the other elements of IO?

b. **Tasks.** What are the individual EW tasks and responsibilities for each component or subdivision of the force? Include all instructions unique to that component or subdivision.

c. **Coordinating Instructions**

- What instructions, if any, are applicable to two or more components or subdivisions?
- What are the requirements, if any, for the coordination of EW actions between subordinate elements?
- What is the guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered elsewhere in this tab?
- What is the emissions control guidance? Place detailed or lengthy guidance in an exhibit to this tab.

- What coordination with the J-6 is required to accomplish the JRFL?

4. Administration and Logistics

a. **Administration**

- What, if any, administrative guidance is required?

- What, if any, reports are required? Include example(s).

b. **Logistics.** What, if any, are the special instructions on logistic support for EW operations?

5. Command and Control

a. **Feedback**

- What is the concept for monitoring the effectiveness of EW operations during execution?

- What are specific intelligence requirements for feedback?

b. **After-Action Reports.** What are the requirements for after-action reporting?

c. **Signal.** What, if any, are the special or unusual EW-related communications requirements?

ANNEX C TO APPENDIX B
JOPES IO (OPERATIONS SECURITY) GUIDANCE

The guidance in this annex relates to the development of Tab C (Operations Security) of Appendix 3 (Information Operations) to Annex C (Operations) of the OPLAN/CONPLAN/OPORD/campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **Enemy Forces**

- **Current Enemy Intelligence Assessment**

  •• What is the estimated enemy's assessment of friendly operations, capabilities, and intentions?

  •• What is the known enemy knowledge of the friendly operation addressed in the basic plan?

- **Enemy Intelligence Capabilities**

  •• What are the enemy's intelligence collection capabilities according to major categories (signals intelligence, HUMINT, imagery intelligence)?

  •• What potential sources (including other nations) provide support to the enemy?

  •• How does the enemy's intelligence system work? Include the time required for intelligence to reach key decision makers.

  •• What are the major analytical organizations and who are the key personalities?

  •• What, if any, unofficial intelligence organizations support the national leadership?

  •• What are the enemy intelligence capabilities strengths and weaknesses?

b. **Friendly Forces**

- **Friendly Operations.** What are the major actions to be conducted by friendly forces in the execution of the basic plan?

- **Critical Information.** What is the identified critical information? Include the critical information of higher headquarters. For phased operations, identify the critical information by phase.

c. **Assumptions.** What are the assumptions upon which this OPSEC plan is based?

2. Mission

What is the OPSEC mission (who, what, when, where, why)?

3. Execution

a. **Concept of Operations**

- What is the role of OPSEC in the commander's IO strategy?

- What is the general concept for the implementation of planned OPSEC measures? Describe these by phase and major activity (maneuver, logistics, communications), if appropriate.

- What will be the OPSEC support to other capabilities or activities?

b. **Tasks.** What are the specific OPSEC measures to be executed? List these by phase and include specific responsibilities for subordinate elements.

c. **Coordinating Instructions**

- What are the requirements for coordination of OPSEC measures between subordinate elements?
- What is the required coordination with public affairs?
- What is the guidance on termination of OPSEC-related activities?
- What is the guidance on declassification and public release of OPSEC-related information?

4. Administration and Logistics

a. What, if any, are the OPSEC-related administrative or logistic support requirements?

b. What, if any, are the administrative- or logistics-related OPSEC measures?

5. Command and Control

a. **Feedback**

- What is the concept for monitoring the effectiveness of OPSEC measures during execution?
- What are the specific intelligence requirements for feedback?

b. **OPSEC Surveys.** What are the plans for conducting OPSEC surveys in support of this operation?

c. **After-Action Reports.** What are the requirements for after-action reporting?

d. **Signal.** What, if any, are the special or unusual OPSEC-related communications requirements?

ANNEX D TO APPENDIX B
JOPES IO (PSYCHOLOGICAL OPERATIONS) GUIDANCE

The guidance in this annex relates to the development of Tab D (Psychological Operations) of Appendix 3 (Information Operations) to Annex C (Operations) of the OPLAN/CONPLAN/OPORD/campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **Overview**

- What is the general psychological situation in the AOR/JOA?
- What, if any, are the ongoing PSYOP programs?
- What are the significant factors influencing PSYOP activities?
- What are the competing PSYOP goals in the AOR/JOA?
- What is the PSYOP task to be accomplished?

b. **US (or US and Allied/Coalition) Perspective**

- How will the assigned PSYOP task be accomplished?
- What resources will be used?
- What will be the general phasing of current actions with future actions?

c. **Neutral Perspective** (if applicable)

- What are the estimated neutral intentions under various circumstances?
- What activities and resources are available to these neutral intentions?
- What neutral actions and behavior would favor mission accomplishment?
- Which apparent current COAs might affect mission accomplishment?
- What resources are available to execute alternative COAs?
- What objective and subjective factors could affect decisions and resource effectiveness?
- What are the staff factions and who are the particularly influential individuals?
- What are the characteristics of decision makers and their key advisors, major staff planners, staff factions (to include particularly influential individuals), and intelligence system analysts?
- What are the groups of related planner and decision maker essential elements of friendly information (EEFI)?
- What is the estimated background knowledge and desired and harmful appreciations for each group?

d. **Enemy Perspectives**

- **Decision Maker and Staff**

  •• Who are the decision makers who can direct development or allocation of resources of COA pertinent to the task assigned?

  •• What feasible alternative actions would favor or harm friendly operational effectiveness?

•• What COAs might affect friendly task accomplishment?

•• What resources are available to execute each COA?

•• What are the characteristics of enemy decision makers, their key advisors, and staff (particularly intelligence analysts)?

- **Intelligence Systems**

•• What are the intelligence systems that support decision makers and their staffs?

•• What are the intelligence systems' capabilities pertinent to the situation?

•• What are the objective and subjective factors and the characteristics of collection planners and decision makers that affect their development and selection for use of information gathering resources?

•• What are the groups of related planner and decision maker EEFI?

•• What is the estimated background knowledge and desired and harmful appreciations for each group?

- **Target Audiences**

•• What groups can influence plans, decisions, and operational effectiveness in task accomplishment?

•• How susceptible are these groups to PSYOP?

•• What group behavior is favorable or harmful to task accomplishment?

•• What are the apparent goals, motivations, and characteristics of each group?

•• Who are the leaders who can cause these groups to behave in various ways?

•• What are the groups of related target audience EEFI?

•• What is the estimated background knowledge and desired and harmful appreciations for each group?

- **Command Systems**

•• What communications systems and command centers will be used to plan COAs and control, coordinate, and supervise execution of the planned COA?

•• What is the purpose and what are the characteristics of each command and control communications net?

•• What are the PSYOP targets for jamming or attacking?

•• When should PSYOP operations to demoralize and disorganize opposing command be executed?

•• When should PSYOP operations to reduce opposing operational effectiveness be executed?

•• When should PSYOP operations to enhance the effectiveness of planned deceptions and PSYOP be executed?

•• When should PSYOP operations to support OPSEC to the maximum advantage be executed?

2. Mission

How will the PSYOP mission support the maneuver commander?

3. Execution

a. **Concept of Operations**

- **Overview**

  •• What is the commander's intent?

  •• What is the overall concept for using PSYOP in support of task accomplishment?

  •• Who will plan and conduct strategic PSYOP in peacetime and in support of pre-conflict deterrence options? Who are the supporting commanders?

  •• Who will plan and conduct strategic and theater PSYOP in support of sustained hostilities? Who are the supporting commanders?

  •• Who will plan and conduct joint tactical PSYOP in support of operational COAs? Who are the supporting commanders?

- **General Guidance to Units and Forces**

  •• What are the valid PSYOP themes to be promoted to induce strategic and theater PSYOP objectives?

  •• What are the valid or invalid PSYOP themes to be discouraged? Include indications of specific target audience sensitivities and harm that might occur if the themes are accepted by target audiences.

  •• **PSYOP Actions Suitable for Use.** (1) What is the guidance for the conduct of military operations, actions, and personnel behavior to promote valid PSYOP themes? (2) What is the guidance for avoiding military operations and actions and personnel behavior that would result in harmful target audience attitudes and behavior? (3) What are the cultural and psychological characteristics of target audiences which will aid operational planners and personnel in selecting COAs and interacting with target audience members?

  •• **Adversary PSYOP.** (1) What adversary PSYOP will be directed at US personnel and at foreign groups in the AOR/JOA. (2) What is the guidance for countering such adversary operations?

- **Outline of Each Planned PSYOP Operation**

  •• What is the target audience and set of PSYOP objectives, overall themes, subgroups to be targeted (to include their characteristics), and specific themes to be promoted for each subgroup?'

  •• What are the provisions for testing, producing, stocking, and disseminating PSYOP materials and for measuring PSYOP effectiveness?

  •• What are the command and staff arrangements? Who are the supporting commanders?

  •• What resources are required to plan and conduct PSYOP actions? Include civil capabilities; indigenous assets; exploitation of enemy prisoners of war (EPWs), internees, and detainees for PSYOP; and military PSYOP resources.

  •• What are the logistics requirements? Include preparation, distribution, and stocking of PSYOP materials; transport of PSYOP material and personnel to operational areas and their basing and support while conducting PSYOP; provisions for the supply and

maintenance of US and indigenous PSYOP material; and fiscal and personnel matters.

•• What are the requirements for implementing schedules and PSYOP operation control sheets?

•• What is the codeword for OPSEC-sensitive PSYOP?

- What is the OPSEC planning guidance? Include planning for, preparing for, and conducting PSYOP and PSYOP actions to maintain essential secrecy for the commander's intention and to gain and maintain essential secrecy for OPSEC-sensitive PSYOP COAs.

b. **Situation Monitoring**

- How will intelligence, multi-discipline CI, security monitoring, and operational feedback be provided?

- What is the requirement for running situation estimates; periodic estimates of target appreciations responsive to EEFI, actions, and attitudes and behavior; and current reporting of intelligence and multi-discipline CI information, security monitoring results, and implementing actions?

- What resources are required? What is their availability?

c. **Control**

- How will control be affected and implementation centrally coordinated?

- What are the coordinating instructions?

- How will implementation planning and supervision of the planned action be accomplished?

- What is the need for specific PSYOP operations?

- What coordination is required with adjacent commands and civilian agencies, to include US diplomatic missions, US Information Agency (USIA), and Agency for International Development?

- What coordination is required with military deception and OPSEC planners, EW planners, and planners in the fields of civic action, FHA, civil affairs, EPWs, CI, detainees, command, control, and communications, legal, captured US personnel, and operations?

d. **Tasks**

- What responsibilities must be assigned to implement the concept?

- Is designation of an executive agent to coordinate implementation among multiple organizations required?

- How will feedback to ensure effectiveness of tasks be provided?

4. Administration and Logistics

a. **Logistics**

- What is the guidance on stocking of PSYOP and information materials and provisions to disseminating organizations?

- What are the provisions for the supply and maintenance of PSYOP-unique supplies and equipment?

- What are the provisions for control and maintenance of indigenous equipment and materials?

- What are the fiscal matters relating to special funds?

- What are the personnel matters relating to indigenous personnel?

b. **Administration**

- What are the requirements for special reports?

- What are the requirements for planning and operations in support of education programs regarding EPWs and civilian internees?

- What will be the participation in interrogation of EPWs, internees, and detainees to obtain information essential or peculiar to PSYOP?

5. Command and Control

Refer to appropriate sections of Annex K (Command, Control, and Communications Systems) and provide pertinent extracts of information included in the basic plan or Annex K, to include the following.

a. What are the recognition and identification instructions?

b. What is the electronic policy?

c. What are the headquarters locations and movements?

d. What are the codewords?

e. What is the frequency allocation?

Intentionally Blank

ANNEX E TO APPENDIX B
JOPES IO (PHYSICAL DESTRUCTION) GUIDANCE

The guidance in this annex relates to the development of Tab E (Physical Destruction) of Appendix 3 (Information Operations) to Annex C (Operations) of the OPLAN/CONPLAN/OPORD/campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **Enemy Situation.** What is the general situation in the target country?

b. **Friendly Situation**

- What is the situation of those friendly forces (higher, adjacent, supporting, and reinforcing) that may affect directly C2 and key infrastructure destruction operations?
- What, if any, are the critical limitations and any other planned IO?

c. **Assumptions.** What, if any, are the assumptions on which this plan is based?

2. Mission

What is the C2 and infrastructure physical destruction mission?

3. Execution

a. **Overview**

- How does the commander visualize the execution of this supporting plan to the IO plan from its beginning to its termination?
- What are the phases of the operation?
- What is the JFC's intent and desired end state?

b. **Tasks for Subordinate Commands.** What are the major tasks of each subordinate command?

c. **Coordinating Instructions.** What are the rules of engagement that impact the C2 and infrastructure destruction plan?

4. Administration and Logistics

a. What are the applicable administrative arrangements, if any, not covered in the basic plan?

b. What are the applicable logistics arrangements, if any, not covered in the basic plan?

5. Command and Control

What are the applicable command and control arrangements, if any, not covered in the basic plan?

Intentionally Blank

ANNEX F TO APPENDIX B
JOPES IO (PUBLIC AFFAIRS) GUIDANCE

The guidance in this annex relates to the development of Annex F (Public Affairs) of the OPLAN/CONPLAN/OPORD/ campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **General.** What are the general responsibilities and guidance for military PA actions (public information/media relations, command and internal information, and community relations)?

b. **Enemy.** What are the expected actions of enemy forces and forces hostile to US interests?

c. **Friendly.** What are the friendly agencies not under JFC control who will contribute to the PA effort? Include Assistant Secretary of Defense (Public Affairs), USIA, US ambassadors, and allied/coalition PA programs.

d. **Policy.** What is the applicable PA policy pertaining to this plan?

e. **Assumptions**

- What are the host-nation preferences and/ or sensitivities to be considered in developing and executing PA programs?
- Should the JFC be prepared to host the DOD National Media Pool during the initial stages of operations?

2. Mission

What are the task and purpose of PA in the operation?

3. Execution

a. **Concept of Operations**

- What PA support will be required in the following five phases.
  - •• Prehostilities
  - •• Lodgment
  - •• Decisive combat and stabilization
  - •• Follow-through
  - •• Posthostilities, including redeployment

b. **Tasks**

- What are the PA tasks to be completed during the above-listed phases?
- What, if any, are the additional information release instructions to the supported combatant commander and other supporting commands, to include release authority and PA guidance on casualty and mortuary affairs, postal affairs, and prisoner of war or missing in action and EPW matters?
- What are PA visual information and combat camera requirements?
- What are the detailed personnel and equipment support requirements to component commands? Include access to the secure voice circuit that connects the Joint Information Bureau (JIB), on-scene commander, supported combatant commander, and the Department of State representative; access to hard copy message facilities between the same

points; and intertheater and intratheater transportation for escorted media.

- What are the Service, component command, and other supporting commands' support requirements?

c. **Coordinating Instructions**

- **Command Relationships.** What are the PA command relationships?

- **Coordination of Release of Information.** What are the detailed procedures for all supporting commands for handling or forwarding to the supported command queries, responses, and proposed news releases for clearance?

- **Other Coordinating Instructions**

  •• What is the guidance for interviews and news conferences with returned US personnel and EPWs or detained personnel?

  •• What is the required PA coordination with other staff elements involved in release of information outside the command?

  •• What are the procedures for keeping PA historical records?

4. Registration

What is the guidance for accreditation of the media?

5. Security Review

What, if any, are the security review procedures?

6. Arrangements for the Media

What are the details on planned media support? Include details concerning messing, billeting, emergency medical treatment, access to transportation and communications facilities at Government expense, access to unclassified operational information, and other support.

a. **Facilities.** What facilities support will be provided to members of the DOD media pool and other media?

b. **Inoculations.** What inoculations will be required for correspondents accompanying troops in the field or embarked on ships of the task forces?

c. **Expenses**

- What services will be provided to the media on a reimbursable basis?

- What are the requirements for reimbursement?

d. **Simulated Rank.** What will be the simulated rank of news media representatives for messing, billeting, and transportation?

e. **Communications.** What will be the procedures for handling media traffic?

f. **Transportation.** What are the procedures for transporting media personnel into, out of, and within the AOR/JOA?

g. **Travel Orders.** What are the procedures for authorizing and issuing travel orders to correspondents.

h. **Pools.** What are the detailed procedures for media participation in media pools?

7. Security of Operations and Personnel

a. **Operations.** What are the guidelines to follow when correspondents are present in the operating areas? Include a balance between security and providing information to the public. Diplomatic and political considerations of all statements and news releases to media representatives should be weighed carefully at all echelons of command.

b. **Personnel**

- **Personal Security.** What personal security measures apply to correspondents in the operating areas?
- **Physical Security.** What physical security measures apply to correspondents in the operating areas?

8. Operations Security

What detailed security procedures, if any, are to be followed by PA personnel?

9. Audiovisual and Visual Information

What are the guidelines that apply to providing PA, audiovisual, and visual information coverage of the operation?

10. Internal Information

What are the internal information requirements for subordinate and component commands?

11. Community Relations

What, if any, coordination is required with Office of the Assistant Secretary of Defense (Public affairs) or designated representative?

NOTE: Additional appendices to Annex F (Public Affairs) of the OPLAN/CONPLAN/OPORD/functional plan may be required as shown below. Detailed instructions for the preparation of these exhibits is in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

Appendices:

1 — Personnel Requirements for JIBs and Sub-JIBs

2 — Equipment and Support Requirements for JIBs and Sub-JIBs

3 — General Ground Rules for the Media

4 — DOD National Media Pool

Intentionally Blank

ANNEX G TO APPENDIX B
JOPES IO (CIVIL AFFAIRS) GUIDANCE

The guidance in this annex relates to the development of Annex G (Civil Affairs) of the OPLAN/CONPLAN/OPORD/ campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **General**

- What is the legal basis for CA activities in this operation?
- What is the expected scope of CA activities in this operation? Include the identification of pertinent international and civil-military agreements.
- What is the purpose of this annex? Normally, the purpose is to provide instructions for guiding all relationships between the military force and civil authorities and inhabitants in the operational area.

b. **Enemy**

- What is the impact of enemy capabilities and probable COAs on the CA situation? Include particular emphasis on identifying requirements for CA functions and activities.
- What is the expected CA situation? Include government institutions, customs and attitudes of the population, and availability of indigenous resources.

c. **Friendly**

- What are the CA functions to be performed by civilian authorities of the United States and friendly governments in the operational area?
- What local indigenous assets are available to support and assist in CA activities?

d. **Assumptions.** What are the basic assumptions on which CA planning is based? Include attention to enemy COAs, availability of indigenous resources, conclusion of necessary agreements with foreign governments on forces.

2. Mission

What is the mission to be accomplished by CA activities in support of the operations envisaged in the basic plan?

3. Execution

a. **Concept of Operations**

- Operations not involving the establishment of a military government.

  •• What are the operational variations due to alternate COAs in the basic plan?

  •• What will be CA support of flexible deterrent options?

  •• Do CA activities support time-phasing of the operation?

  •• What will be the deployment and employment of forces to support CA operations?

  •• What will be the scope and duration of CA operations? Include postconflict CA operations.

•• What are the desired end states in CA activities? These should be clear, concise, and subdivided as necessary to describe the successful completion of each phase and COA.

•• What is the planned allocation and use of military units and resources for the performance of CA functions?

•• What are the principal CA functions to be performed within the command area? Include any significant variations by country, state, or region.

•• What will be the function and operation of civil-military operations centers, if they are established?

- Operations involving the establishment of a military government.

•• What is the constructive or restrictive guidance on each CA functional area?

•• What CA authorities are required?

•• What additional CA coordination is required?

b. **Tasks.** What are the specific tasks assigned to each element of the supported and supporting commands? Each task should be a concise statement of a mission to be performed either in future planning for the operation or on execution of the OPORD and must include all key elements required for CA functions.

c. **Coordinating Instructions**

- What are the instructions applicable to the whole command; two or more elements of the command; and the command or its elements and agencies external to the command?

- What, if any, are the established CA boundaries?

- What, if any, are the liaison arrangements with allied/coalition forces and between subordinate commands?

- What are the claims policies? See also legal appendix to Annex E.

- What is the application or negotiation of status-of-forces agreements? See also legal appendix to Annex E.

- What is the required liaison and coordination with USG and nongovernment agencies? See also legal appendix to Annex E.

- What proclamations are to be issued to the civil populace in coordination with the legal appendix to Annex E?

- What is the required liaison and coordination with host country or other friendly countries and government and nongovernment agencies?

- What are the emergency measures, if any, for defense of civil populations?

- What will be the PSYOP support to CA operations?

4. Administration and Logistics

a. **Military Resource Requirements.** What, if any, are the applicable requirements to maintain military equipment and supplies for support of the CA function?

b. **Civilian Personnel.** What is the estimated local civilian labor required and available to support the operation?

c. **Civilian Facilities and Supplies.** What are the estimated local civilian facilities and supplies required and available to support the operation?

d. **Reports.** What, if any, are the administrative reporting requirements?

5. Command and Control

a. What, if any, are the differences between the command channels for the conduct of CA activities and the command relationships established in Annex J.

b. Who has command responsibility for operational control, administrative control, and logistics of CA forces and activities? Emphasize the difference between activities and forces and include any changes or transitions between C2 organizations and the time of the expected shift.

c. What, if any, command arrangement agreements and memorandums of understanding are being used. Which of these, if any, require development?

Intentionally Blank

APPENDIX C
JOPES DEFENSIVE INFORMATION OPERATIONS GUIDANCE

The guidance in this appendix relates to the development of Appendix 2 (Defensive Information Operations) to Annex K (Command, Control, and Communications Systems) of the OPLAN/CONPLAN/OPORD/campaign plan/functional plan format found in CJCSM 3122.03, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance."

1. Situation

a. **General**

- What are the defensive IO objectives?
- How do these objectives relate to mission accomplishment?

b. **Enemy.** What are the enemy capabilities that affect friendly information, and information systems, and IO not already discussed in Annex K?

c. **Friendly.** What are the organizations that are not subordinate to this command and the specific tasks assigned to each supporting defensive IO objective?

2. Mission

How do defensive IO support the accomplishment of the mission assigned in the basic plan?

3. Execution

a. **Concept of Operations**

- **General.** What is the overall concept for ensuring friendly information access and availability despite enemy IO use? Pay particular attention to physical security and survivability of friendly information system capabilities and facilities.

- **Phasing**

  •• What are the defensive IO activities occurring in each operational phase? Describe activity sequences in each phase keyed to phase initiation and supported operational events.

  •• What is the time-phased guidance for accomplishing actions implementing the defensive IO plan?

b. **Tasks**

- What command element is responsible for coordinating defensive IO actions?
- What are the assigned tasks and responsibilities of each subordinate command to implement and accomplish defensive IO actions, to include identification of vulnerabilities?

c. **Coordinating Instructions**

- **Integration**

  •• What are the detailed instructions for accomplishing integration of physical security and survivability measures, electronic warfare, INFOSEC, CI, PA, counter-PSYOP, counter-deception, and OPSEC means of performing defensive IO?

  •• What is the guidance for mitigation and/or negation of adversary capabilities?

- **Coordination.** What are the detailed requirements for coordinating among

elements involved in defensive IO? Emphasize close coordination with IO, C2W, deception, OPSEC, EW, PSYOP, intelligence, PA, and other key planners that rely on friendly information resources.

- **Security.** What, if any, are the special security or handling requirements for defensive IO planning and actions envisaged by this appendix?

- **Reports.** What, if any, are the operational reporting requirements necessary for effective monitoring of defensive IO activities?

4. Administration and Logistics

a. **Personnel.** What, if any, are the requirements for specialized personnel qualifications and/or qualification?

b. **Supply.** What, if any, are the specialized equipment supply requirements?

c. **Reports.** What, if any, are the required administrative reports?

5. Command and Control

What special systems or procedures, if any, are required for C2 of defensive IO actions?

APPENDIX D
REFERENCES

The development of Joint Pub 3-13 is based upon the following primary references:

1. Unified Command Plan (UCP).

2. DODD S-3600.1, "Information Operations (IO) (U)."

3. DODI S-3600.2, "Information Warfare Security Classification Instruction (U)."

4. CJCS MOP 10, "Near-Real-Time Analysis of Electromagnetic Interference and Jamming to US Space Systems."

5. CJCSI 3110.01B, "Joint Strategic Capabilities Plan."

6. CJCSI 3170.01, "Requirements Generation System."

7. CJCSI 3210.01A, "Joint Information Operations Policy."

8. CJCSI 3210.03, "Joint Electronic Warfare Policy."

9. CJCSI 3220.01, "Electromagnetic Spectrum Use in Joint Military Operations."

10. CJCSI 3220.02, "Joint Spectrum Interference Resolution (JSIR)."

11. CJCSI 5118.01, "Charter for the Joint Command and Control Warfare Center."

12. CJCSI 6510.01B, "Defensive Information Operations Implementation."

13. CJCSM 3122.03, "Joint Operations Planning and Execution System, Volume II, Planning Formats and Guidance."

14. Joint Pub 1, "Joint Warfare of the Armed Forces of the United States."

15. Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

16. Joint Pub 1-01, "Joint Publication System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program."

17. Joint Pub 1-02, "DOD Dictionary of Military and Associated Terms."

18. Joint Pub 2-0, "Doctrine for Intelligence Support to Joint Operations."

19. Joint Pub 2-01, "Joint Intelligence Support to Military Operations."

20. Joint Pub 2-01.1, “Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting.”

21. Joint Pub 2-01.2, “Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations.”

22. Joint Pub 2-01.3, “Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.”

23. Joint Pub 2-02, “National Intelligence Support to Joint Operations.”

24. Joint Pub 3-0, “Doctrine for Joint Operations.”

25. Joint Pub 3-05, “Doctrine for Joint Special Operations.”

26. Joint Pub 3-13.1, “Joint Doctrine for Command and Control Warfare (C2W).”

27. Joint Pub 3-16, “Joint Doctrine for Multinational Operations.”

28. Joint Pub 3-51, “Electronic Warfare in Joint Military Operations.”

29. Joint Pub 3-52, “Doctrine for Joint Airspace Control in the Combat Zone.”

30. Joint Pub 3-53, “Doctrine for Joint Psychological Operations.”

31. Joint Pub 3-54, “Joint Doctrine for Operations Security.”

32. Joint Pub 3-55, “Doctrine for Reconnaissance, Surveillance, and Target Acquisition (RSTA) Support for Joint Operations.”

33. Joint Pub 3-56.1 “Command and Control for Joint Air Operations.”

34. Joint Pub 3-57, “Doctrine for Joint Civil Affairs.”

35. Joint Pub 3-58, “Joint Doctrine for Military Deception.”

36. Joint Pub 3-61, “Doctrine for Public Affairs in Joint Operations.”

37. Joint Pub 4-0, “Doctrine for Logistic Support of Joint Operations.”

38. Joint Pub 5-0, “Doctrine for Planning Joint Operations.”

39. Joint Pub 5-00.2, “Joint Task Force Planning Guidance and Procedures.”

40. Joint Pub 6-0, “Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations.”

41. Joint Pub 6-02, "Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems."

42. Chief of Naval Operations Instruction 3430.26, "Implementing Instruction for Information Warfare/Command and Control Warfare."

43. Naval Doctrine Publication 6, "Naval Command and Control Warfare."

44. Air Force Doctrine Document 2-5, "Information Operations."

45. US Army Field Manual 100-5, "Operations."

46. US Army Field Manual 100-6, "Information Operations."

47. Marine Corps Order 3430.1, "Policy for Information Operations."

48. Chief of Naval Operations/Commandant of the Marine Corps Memorandum "Information Warfare and Command and Control Warfare (IW/C2W)."

Intentionally Blank

APPENDIX E
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to the Joint Warfighting Center, Attn: Doctrine Division, Fenwick Road, Bldg 96, Fort Monroe, VA 23651-5000. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

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

3. Change Recommendations

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

TO: JOINT STAFF WASHINGTON DC//J3/J39//
INFO: JOINT STAFF WASHINGTON DC//J7-JDD//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, DC 20318-7000.

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

c. Record of Changes:

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

4. Distribution

a. Additional copies of this publication can be obtained through Service publication centers.

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

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

By Military Services:

Army:	US Army AG Publication Center SL 1655 Woodson Road Attn: Joint Publications St. Louis, MO 63114-6181
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Marine Corps Logistics Base Albany, GA 31704-5000
Coast Guard:	Coast Guard Headquarters, COMDT (G-OPD) 2100 2nd Street, SW Washington, DC 20593-0001

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

GLOSSARY

PART I — ABBREVIATIONS AND ACRONYMS

AIS	automated information systems
AOR	area of responsibility
C2	command and control
C2W	command and control warfare
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
CA	civil affairs
CERT	computer emergency response team
CI	counterintelligence
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMO	civil-military operations
CNA	computer network attack
COA	course of action
COMPUSEC	computer security
COMSEC	communications security
CONPLAN	operation plan in concept format
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODD	Department of Defense Directive
EA	electronic attack
EEFI	essential elements of friendly information
EP	electronic protection
EPW	enemy prisoner of war
ES	electronic warfare support
EW	electronic warfare
FDO	flexible deterrent option
FHA	foreign humanitarian assistance
GII	global information infrastructure
HN	host nation
HUMINT	human intelligence
I&W	indications and warning
IA	information assurance
INFOSEC	information security

IO	information operations
IPB	intelligence preparation of the battlespace
IW	information warfare
J-2	Intelligence Directorate of a joint staff
J-3	Operations Directorate of a joint staff
J-4	Logistics Directorate of a joint staff
J-5	Plans Directorate of a joint staff
J-6	Command, Control, Communications, and Computer Systems Directorate of a joint staff
J-7	Operational Plans and Interoperability Directorate of a joint staff
JC2WC	Joint Command and Control Warfare Center
JCCC	joint communications control center
JCMA	Joint COMSEC (communications security) Monitoring Activity
JCSE	Joint Communications Support Element
JFC	joint force commander
JIB	Joint Information Bureau
JOA	joint operations area
JOC	joint operations center
JOPES	Joint Operation Planning and Execution System
JPG	joint planning group
JPO-STC	Joint Program Office for Special Technology Countermeasures
JPOTF	joint psychological operations task force
JRFL	joint restricted frequency list
JSC	Joint Spectrum Center
JTCB	joint targeting coordination board
JTF	joint task force
JWAC	Joint Warfare Analysis Center
LOC	line of communications
M&S	modeling and simulation
MOOTW	military operations other than war
NCA	National Command Authorities
NGO	nongovernmental organization
NII	National Information Infrastructure
NSA	National Security Agency
OPFOR	opposition force
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PA	public affairs
PSYOP	psychological operations

ROE	rules of engagement
SIO	special information operations
SOF	special operations forces
STO	special technical operations
USG	United States Government
USIA	United States Information Agency

civil affairs. The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local 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. Also called CA. (Joint Pub 1-02)

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

command and control warfare. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. (This term and its definition modifies the existing term and its definition and are approved for inclusion in the next edition of Joint Pub 1-02.)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. a. cryptosecurity — The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. transmission security — The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. emission security — The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. physical security — The component of communications security that results from all physical measures necessary to safeguard classified equipment, material,

and documents from access thereto or observation thereof by unauthorized persons. (Joint Pub 1-02)

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

computer security. The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. Also called COMPUSEC. (Joint Pub 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. (Joint Pub 1-02)

counterintelligence. 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. Also called CI. (Joint Pub 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1-02)

Defense Information Infrastructure. The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The Defense Information Infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. Also called DII. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

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

directed-energy warfare. Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. (Joint Pub 1-02)

electronic warfare. 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, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. 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, or antiradiation weapons). b. electronic protection. That division of electronic warfare involving actions 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 sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate 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, both communications intelligence, and electronic intelligence. (Joint Pub 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. Also called GII. (This term and its definition modifies the existing term and definition and are approved for inclusion in the next edition of Joint Pub 1-02.)

incident. In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

indications and warning. Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied/coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or

intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied/coalition nations; hostile reactions to US reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (This term and its definition modifies the existing term and definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

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. (Joint Pub 1-02)

information assurance. 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. Also called IA. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

information-based processes. Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

information security. Information security is the protection and defense 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. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02).

information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (This term and its definition modifies the existing term and definition and are approved for inclusion in the next edition of Joint Pub 1-02.)

information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (This term and its definition modifies the existing term and definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called

IW. (This term and its definition modifies the existing term and definition and will be included in Joint Pub 1-02.)

intelligence preparation of the battlespace. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (Joint Pub 1-02)

leveraging. In information operations, the effective use of information, information systems, and technology to increase the means and synergy in accomplishing information operations strategy. (This term and its definition modifies the existing term and definition and will be included in the next edition of Joint Pub 1-02.)

military deception. Actions executed to deliberately mislead adversary military decisionmakers 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. The five categories of military deception are: a. strategic military deception — Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations. b. operational military deception — Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations. c. tactical military deception — Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. d. Service military deception — Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems. e. military deception in support of operations security (OPSEC) — Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities. (Joint Pub 1-02)

military operations other than war. Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and occur before, during, and after war. Also called MOOTW. (Joint Pub 1-02)

national information infrastructure. The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national 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 national information infrastructure. Also called NII. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

operational level of war. The level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics; they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives. (Joint Pub 1-02)

operations security. 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 hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

perception management. Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and 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. (Joint Pub 1-02)

physical security. 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. (Joint Pub 1-02)

probe. In information operations, any attempt to gather information about an automated information system or its on-line users. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

psychological operations. 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. Also called PSYOP. (Joint Pub 1-02)

public affairs. Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA. (Joint Pub 1-02)

special information operations. Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. Also called SIO. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

strategic level of war. The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) security objectives and guidance, and develops and uses national resources to accomplish these objectives. Activities at this level establish national and multinational military objectives; sequence initiatives; define limits and assess risks for the use of military and other instruments of national power; develop global plans or theater war plans to achieve these objectives; and provide military forces and other capabilities in accordance with strategic plans. (Joint Pub 1-02)

tactical level of war. The level of war at which battles and engagements are planned and executed to accomplish military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives. (Joint Pub 1-02)

vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (This term and its definition modifies the existing term and definition and are approved for inclusion in the next edition of Joint Pub 1-02.)

vulnerability analysis. In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)