Joint Publication 3-13

Information Operations

13 February 2006

PREFACE

1. Scope

This publication provides doctrine for information operations planning, preparation, execution, and assessment in support of joint operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in operations and provides the doctrinal basis for interagency coordination and for US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for 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 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 objective.

3. Application

a. Joint doctrine established in this publication applies to the commanders of combatant commands, subunified commands, joint task forces, subordinate components of these commands, and the Services.

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 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 and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-13
DATED 9 OCTOBER 1998

- **Aligns joint information operations (IO) doctrine with the transformational planning guidance as specified by the 30 October 2003 Department of Defense Information Operations Roadmap**
- **Discontinues use of the terms "offensive IO" and "defensive IO" but retains the recognition that IO is applied to achieve both offensive and defensive objectives**
- **Removes information warfare as a term from joint IO doctrine**
- **Updates the descriptions and interrelationship of the five core IO capabilities (electronic warfare, computer network operations, psychological operations, operations security, and military deception) and their associated supporting and related capabilities**
- **Establishes the core capability of computer network operations, consisting of computer network attack, computer network defense, and computer network exploitation**
- **Adds combat camera and realigns physical attack, information assurance, and counterintelligence under supporting IO capabilities**
- **Adds defense support to public diplomacy and realigns public affairs and civil military operations under related IO capabilities**
- **Adds a description of the information environment and discusses its relationship to IO and other military operations**
- **Adds a discussion of the relationship of IO to strategic communication**
- **Adds a separate chapter on intelligence and communications system support to IO**
- **Expands the chapter on IO planning to address IO considerations in joint planning, situational aspects of IO planning, IO measures of performance and effectiveness, and the importance of interagency coordination in IO planning**
- **Adds a discussion on the planning aspects of IO and theater security cooperation planning**
- **Adds a separate chapter on multinational considerations in IO**

Intentionally Blank

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY ix

CHAPTER I
INTRODUCTION

- Introduction I-1
- The Information Environment I-1
- Military Operations and the Information Environment I-3
- Principles of Information Operations I-6
- Strategic Communication I-10
- Importance of Information Operations in Military Operations I-10

CHAPTER II
CORE, SUPPORTING, AND RELATED INFORMATION
OPERATIONS CAPABILITIES

- Introduction II-1
- Core Information Operations Capabilities II-1
- Information Operations Supporting Capabilities II-5
- Information Operations Related Capabilities II-8

CHAPTER III
INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS

- Introduction III-1
- Intelligence Support to Information Operations III-1

CHAPTER IV
RESPONSIBILITIES AND COMMAND RELATIONSHIPS

- Introduction IV-1
- Authorities and Responsibilities IV-1
- Joint Information Operations Organizational Roles and Responsibilities IV-2
- Organizing for Joint Information Operations IV-3

CHAPTER V
PLANNING AND COORDINATION

- Introduction V-1
- Information Operations Planning V-1
- Information Operations Planning Considerations V-2

- Commander's Intent and Information Operations V-7
- The Relationship Between Measures of Performance and Measures of Effectiveness V-7

CHAPTER VI
MULTINATIONAL CONSIDERATIONS IN INFORMATION OPERATIONS

- Introduction VI-1
- Other Nations and Information Operations VI-1
- Multinational Information Operations Considerations VI-2
- Planning, Integration, and Command and Control of Information Operations in Multinational Operations VI-3
- Multinational Organization for Information Operations Planning VI-3
- Multinational Policy Coordination VI-3

CHAPTER VII
INFORMATION OPERATIONS IN JOINT EDUCATION, TRAINING, EXERCISES, AND EXPERIMENTS

- Introduction VII-1
- Information Operations Education VII-1
- Information Operations Training VII-2
- Planning Information Operations in Joint Exercises VII-3
- Information Operations Exercise Preparation, Execution, and Post-Exercise Evaluation VII-7
- Information Operations in Joint Experimentation VII-8

APPENDIX

A Supplemental Guidance (published separately) A-1
B Mutual Support Between Information Operations Core Capabilities B-1
C Communications System Support to Information Operations C-1
D References D-1
E Administrative Instructions E-1

GLOSSARY

Part I Abbreviations and Acronyms GL-1
Part II Terms and Definitions GL-4

FIGURE

I-1 The Information Environment I-2
I-2 Information Quality Criteria I-3
I-3 Information Operations Integration into Joint Operations (Notional) I-7

II-1 Principles of Public Information II-9
IV-1 Information Operations Cell Chief Functions IV-4
IV-2 Notional Information Operations Cell IV-5
V-1 Information Operations Cell Actions and Outcomes as Part of Joint Planning V-4
V-2 Example of the Relationship Between Measures of Performance and Measures of Effectiveness V-8
B-1 Mutual Support Within Information Operations Capabilities B-1
B-2 Potential Conflicts Within the Capabilities of Information Operations B-5
B-3 Support Roles of Information Operations, Civil-Military Operations, Public Affairs, Defense Support to Public Diplomacy, and Combat Camera B-8

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

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

Military Operations and the Information Environment

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

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

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

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

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

Core, Supporting, and Related Information Operations Capabilities

Core capabilities.

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

Supporting capabilities.

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

Related capabilities.

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

Intelligence and Communications System Support to Information Operations

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

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

Nature of IO intelligence requirements.

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

Intelligence considerations in planning IO.

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

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

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

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

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

Responsibilities and Command Relationships

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

Combatant commands. Commander, United States Strategic Command's (USSTRATCOM's) specific authority and responsibility to coordinate IO across area of responsibility (AOR) and functional boundaries does not diminish **the imperative for other combatant commanders to employ IO**. These efforts may be directed at achieving national or military objectives incorporated in theater security cooperation plans, shaping the operational environment for potential employment during periods of heightened tensions, or in support of specific military operations. It is entirely possible that in a given theater, the combatant commander will be supported for select IO while concurrently supporting USSTRATCOM IO activities across multiple theater boundaries.

Components. **Components** are normally responsible for detailed planning and execution of IO. IO planned and conducted by functional components must be conducted within the parameters established by the JFC. At the same time, component commanders and their subordinates must be provided sufficient flexibility and authority to respond to local variations in the information environment. Component commanders determine how their staffs are organized for IO, and normally designate personnel to liaise between the JFC's headquarters and component headquarter staffs.

Subordinate joint force commanders.

Subordinate JFCs plan and execute IO as an integrated part of joint operations. Subordinate staffs normally share the same type of relationship with the parent joint force IO staff as the Service and functional components. **Subordinate JFC staffs may become involved in IO planning and execution to a significant degree**, to include making recommendations for employment of specific capabilities, particularly if most of the capability needed for a certain operation resides in that subordinate joint task force.

Organizing for joint IO.

Combatant commanders normally **assign responsibility for IO** to the **J-3**. When authorized, the director of the J-3 has primary staff responsibility for planning, coordinating, integrating, and assessing joint force IO. **The J-3 normally designates an IO cell chief** to assist in executing joint IO responsibilities. The primary function of the IO cell chief is to ensure that IO are integrated and synchronized in all planning processes of the combatant command staff and that IO aspects of such processes are coordinated with higher, adjacent, subordinate, and multinational staffs. To integrate and synchronize the core capabilities of IO with IO-supporting and related capabilities and appropriate staff functions, the IO cell chief normally leads an "IO cell" or similarly named group as an integrated part of the staff's operational planning group or equivalent. The organizational relationships between the joint IO cell and the organizations that support the IO cell are per JFC guidance.

Planning and Coordination

IO planning follows the same principles and processes established for joint operation planning.

The IO staff coordinates and synchronizes capabilities to accomplish JFC objectives. Uncoordinated IO can compromise, complicate, negate, or harm other JFC military operations, as well as other USG information activities. JFCs must ensure IO planners are fully integrated into the planning and targeting process, assigning them to the joint targeting coordination board in order to ensure full integration with all other planning and execution efforts. Other USG and/or coalition/allied information activities, when uncoordinated, may complicate, defeat, or render DOD IO ineffective. Successful execution of an information strategy also requires early detailed JFC IO staff planning, coordination, and deconfliction with USG interagency efforts in the AOR to effectively synergize and integrate IO capabilities.

Planning considerations.

IO planning must begin at the **earliest stage** of a JFC's campaign or operations planning and must be an integral part of, not an addition to, the overall planning effort. IO are used in all phases of a campaign or

operation. The use of IO during early phases can significantly influence the amount of effort required for the remaining phases.

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

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

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

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

Commander's intent and information operations.

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

Measures of performance and measures of effectiveness.

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

Multinational Considerations in Information Operations

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

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

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

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

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

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

IO education considerations.

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

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

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

IO training considerations.

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

IO training must support the IO career force and be consistent with the joint assignment process. Joint IO training focuses on joint planning-specific skills, methodologies and tools, and assumes a solid foundation of Service-level IO training.

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

CONCLUSION

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

CHAPTER I
INTRODUCTION

"The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew."

Abraham Lincoln, Message to Congress 1 December 1862

1. Introduction

Information operations (IO) are integral to the successful execution of military operations. A key goal of IO is to achieve and maintain information superiority for the US and its allies. Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior decisions. IO are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. The purpose of this doctrine is to provide joint force commanders (JFCs) and their staffs guidance to help prepare, plan, execute, and assess IO in support of joint operations. To apply IO across the range of military operations, the JFC integrates his military actions, forces, and capabilities throughout the domains (air, land, sea, and space) of the operating environment in order to create and/or sustain desired and measurable effects on adversary leaders, forces (regular or irregular), information, information systems, and other audiences; while protecting and defending the JFC's own forces actions, information, and information systems. The commander assesses the nature of the mission and develops the intent for IO in all phases of an operation or campaign.

2. The Information Environment

a. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The actors include leaders, decision makers, individuals, and organizations. Resources include the materials and systems employed to collect, analyze, apply, or disseminate information. The information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision making. Even though the information environment is considered distinct, it resides within each of the four domains. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive (see Figure I-1).

(1) **The Physical Dimension.** The physical dimension is composed of the command and control (C2) systems, and supporting infrastructures that enable individuals and organizations to conduct operations across the air, land, sea, and space domains. It is also the dimension where physical platforms and the communications networks that connect them reside. This includes the means of transmission, infrastructure, technologies, groups, and populations. Comparatively, the elements of this dimension are the easiest to measure, and consequently, combat power has traditionally been measured primarily in this dimension.

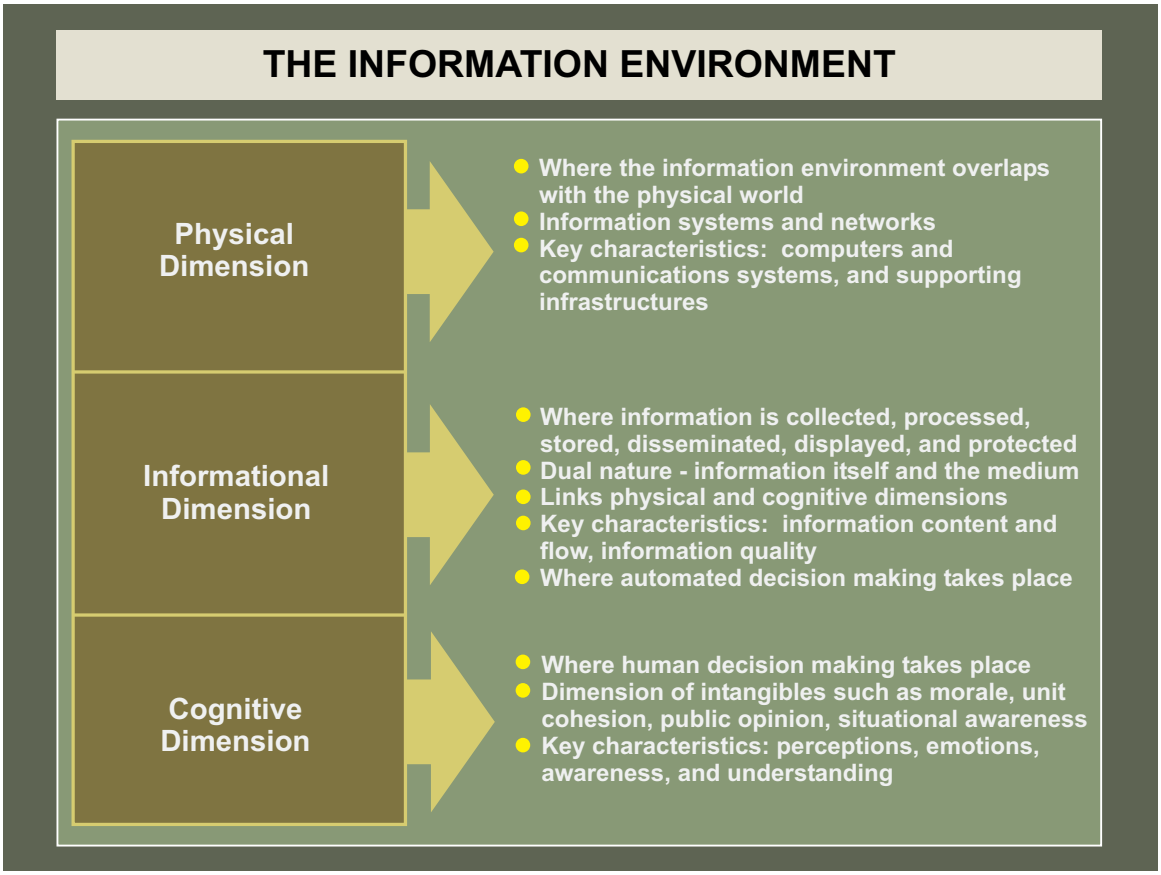


Figure I-1. The Information Environment

(2) **The Informational Dimension.** The informational dimension is where information is collected, processed, stored, disseminated, displayed, and protected. It is the dimension where the C2 of modern military forces is communicated, and where commander's intent is conveyed. It consists of the content and flow of information. Consequently, it is the informational dimension that must be protected.

(3) **The Cognitive Dimension.** The cognitive dimension encompasses the mind of the decision maker and the target audience (TA). This is the dimension in which people think, perceive, visualize, and decide. It is the most important of the three dimensions. This dimension is also affected by a commander's orders, training, and other personal motivations. Battles and campaigns can be lost in the cognitive dimension. Factors such as leadership, morale, unit cohesion, emotion, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information, and rumors influence this dimension.

b. **Advancements in technology have enabled information to be collected, processed, stored, disseminated, displayed, and protected outside the cognitive process in quantities and at speeds that were previously incomprehensible.** While technology makes great quantities of information available to audiences worldwide, perception-affecting factors provide the context which individuals use to translate data into information and knowledge.

c. **There are criteria that define the quality of information relative to its purpose.** Information quality criteria are shown in Figure I-2. The varying purposes of information require different applications of these criteria to qualify it as valuable. Additionally, each decision relies on a different weighting of the information quality criteria to make the best decision.

d. **The finite amount of time and resources available to obtain information must be considered.** Whether decisions are made cognitively or pre-programmed in automated systems, the limited time and resources to improve the quality of available information leaves decision making subject to manipulation. Additionally, there are real costs associated with obtaining quality information — that is, information well-suited to its purpose —such as those to acquire, process, store, transport, and distribute information. The overall impact of successful IO improves the quality of friendly information while degrading the quality of adversary information, thus, providing friendly forces the ability to make faster, more accurate decisions. Quality criteria are shown in Figure I-2.

3. Military Operations and the Information Environment

a. **Information is a strategic resource vital to national security.** Dominance of the information environment is a reality that extends to the Armed Forces of the US at all levels. Military operations, in particular, are dependent on many simultaneous and integrated activities that, in turn, depend on information, and information systems, which must be protected.

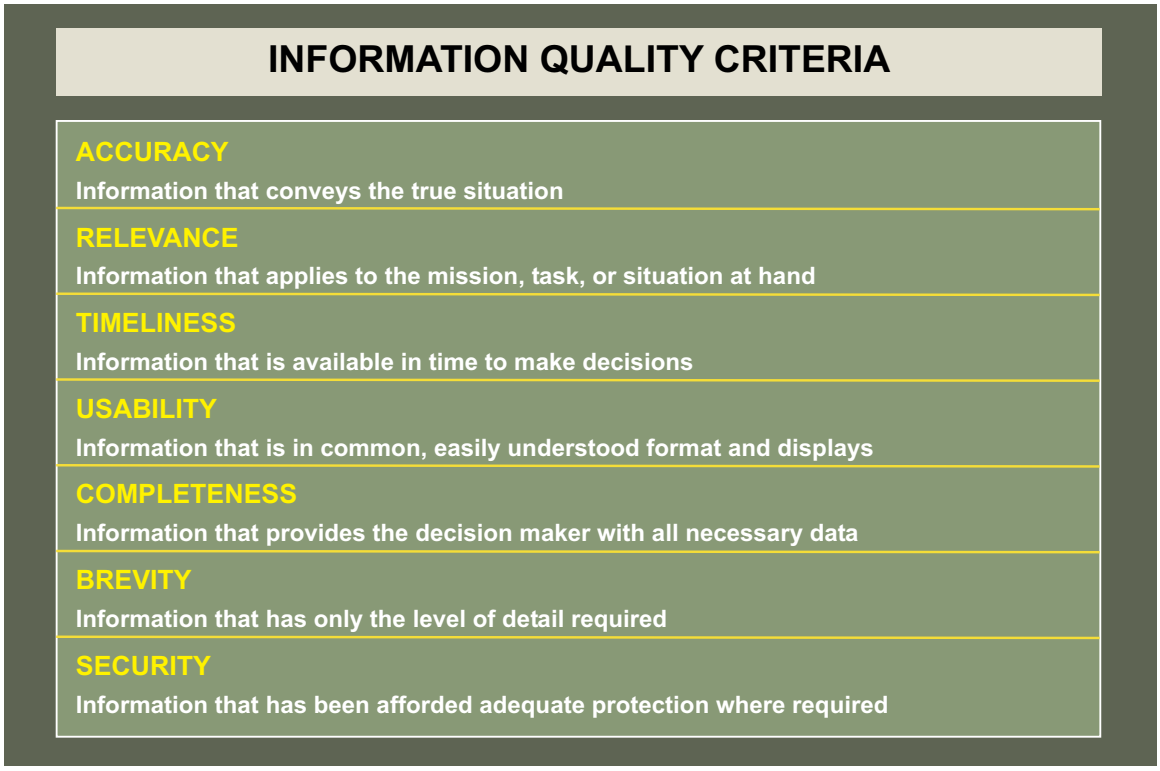


Figure I-2. Information Quality Criteria

b. **In modern military operations, commanders face a variety of information challenges.** Technical challenges include establishing and maintaining connectivity, particularly in austere and distributed locations. Operational challenges include the complexities of modern combat against adversaries with growing information capabilities. For example, regardless of their size, adversaries, including terrorist groups, can counter US efforts through propaganda campaigns, or develop, purchase, or download from the Internet tools and techniques enabling them to attack US information and information systems which may result in tangible impacts on US diplomatic, economic, or military efforts. The global information environment and its associated technologies is potentially available to everyone and as a result, US military commanders face another challenge. Our adversaries now have the capability to pass information, coordinate, exchange ideas, and synchronize their actions instantaneously.

c. The commander visualizes, plans, and directs operations — IO are a part of those operations. The commander's intent should specify a visualization of the desired effects to be achieved with IO and other operations for the staff to develop IO objectives. The commander must not only be able to visualize the desired effects to be achieved with IO but also understand the adversary's capabilities to limit the impact of US operations while the adversary strives to acquire information superiority from the US. These effects can vary based on the objectives of the mission, ranging from disrupting an enemy commander in combat to assuring friendly nations through combined/multinational military training/exercises during peacetime. The role of the military and the desired end state or effect, is dependent on the nature of the conflict. If conducting a humanitarian assistance mission, then generating goodwill for the services rendered and departing with a favorable impression of US activities becomes a primary objective. The commander's intent must include the concept of how these effects will help achieve force objectives.

d. **Military forces operate in an information environment of constantly changing content and tempo.** This evolution adds another layer of complexity to the challenge of planning and executing military operations at a specific time and in a specific location. A continuum of long-, medium-, and short-term factors shape the information environment for which military operations are planned and in which such operations are executed. Commanders and IO cell chiefs must be prepared to adapt or modify IO plans to meet their desired IO effects.

(1) Long-term factors which may shape the information environment include the various ways by which humans:

(a) Organize (nation states, tribes, families, etc.).

(b) Govern.

(c) Interact as groups (culture, sociology, religion, etc.).

(d) Are regionally influenced (stability, alliances, economic relationships, etc.).

(e) Are technologically advanced.

(2) Medium-term factors may include the rise and fall of leaders, competition between groups over resources or goals, incorporation of specific technologies into information infrastructure; and the employment of resources by organizations to take advantage of information technology and infrastructure.

(3) Short-term factors may include weather; availability of finite resources to support or employ specific information technologies (ITs); and ability to extend/maintain sensors and portable information infrastructure to the specific location of distant military operations.

e. The pervasiveness of the information environment in human activity combined with the speed and processing power of modern IT enhances and complicates military efforts to organize, train, equip, plan, and operate. Today, technology has opened the way to an ever-increasing span of control.

f. **US forces perform their missions in an increasingly complex information environment**. To succeed, it is necessary for US forces to gain and maintain information superiority. In Department of Defense (DOD) policy, information superiority is described as the operational advantage gained by the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

(1) The forces possessing better information and using that information to more effectively gain understanding have a major advantage over their adversaries. A commander who gains this advantage can use it to accomplish missions by affecting perceptions, attitudes, decisions, and actions. However, information superiority is not static; during operations, all sides continually attempt to secure their own advantages and deny useful information to adversaries. The operational advantages of information superiority can take several forms, ranging from the ability to create a common operational picture to the ability to delay an adversary's decision to commit reinforcements.

(2) Recognizing information superiority can be difficult to attain over certain adversaries, but its advantages are significant. When it exists, the information available to commanders allows them to accurately visualize the situation, anticipate events, and make appropriate, timely decisions more effectively than adversary decision makers. In essence, information superiority enhances commanders' freedom of action and allows them to execute decisions, and maintain the initiative, while remaining inside the adversary's decision cycle. However, commanders recognize that without continuous IO designed to achieve and maintain information superiority, adversaries may counter those advantages and possibly attain information superiority themselves. Commanders can achieve information superiority by maintaining accurate situational understanding while controlling or affecting the adversaries' or TAs' perceptions. The more a commander can shape this disparity, the greater the friendly advantage.

g. Potential information adversaries come in many shapes: traditionally hostile countries who wish to gain information on US military capabilities and intentions; malicious hackers who wish to steal from or harm the US Government (USG) or military; terrorists; and economic competitors, just to name a few. Potential adversarial information attack techniques are numerous. Some, particularly electronic means, can be prevented by the consistent application of encryption, firewalls, and other network security techniques. Others are considerably more difficult to counter. Possible threat information

techniques include, but are not limited to, deception, electronic attack (EA), computer network attack (CNA), propaganda and psychological operations, and supporting signals intelligence (SIGINT) operations.

h. With the free flow of information present in all theaters, such as television, phone, and Internet, conflicting messages can quickly emerge to defeat the intended effects. As a result, continuous synchronization and coordination between IO, public affairs (PA), public diplomacy (PD), and our allies is imperative, and will help ensure that information themes employed during operations involving neutral or friendly populations remain consistent.

i. **Legal Considerations in IO. IO may involve complex legal and policy issues requiring careful review.** Beyond strict compliance with legalities, US military activities in the information environment as in the physical domains, are conducted as a matter of policy and societal values on a basis of respect for fundamental human rights. US forces, whether operating physically from bases or locations overseas or from within the boundaries of the US or elsewhere, are required by law and policy to act in accordance with US law and the law of armed conflict (LOAC).

4. Principles of Information Operations

a. Success in military operations depends on collecting and integrating essential information while denying it to the adversary and other TAs. IO encompass planning, coordination, and synchronization of the employment of current capabilities to deliberately affect or defend the information environment to achieve the commander's objectives. Figure I-3 describes how IO is integrated into joint operations.

(1) **Core capabilities** (EW, CNO, PSYOP, MILDEC, and OPSEC) are integrated into the planning and execution of operations in the information environment.

(2) **Supporting IO capabilities** (information assurance [IA], physical security, physical attack, counterintelligence [CI], and combat camera [COMCAM]) have military purposes other than IO but either operate in the information environment or have impact on the information environment.

(3) **Related IO capabilities** (PA, civil-military operations [CMO], and defense support to public diplomacy [DSPD]) may be constrained by US policy or legal considerations. While these capabilities have common interfaces with IO, their primary purposes and rules make them separate and distinct. As a result, it is essential that commanders and their staffs coordinate their efforts when exercising their functions within the information environment.

b. **IO are primarily concerned with affecting decisions and decision-making processes, while at the same time defending friendly decision-making processes**. Primary mechanisms used to affect the information environment include: influence, disruption, corruption, or usurpation.

INFORMATION OPERATIONS INTEGRATION INTO JOINT OPERATIONS (NOTIONAL)

Core, Supporting, Related Information Activities	Activities	Audience/ Target	Objective	Information Quality	Primary Planning/ Integration Process	Who does it?
Electronic Warfare	Electronic Attack	Physical, Informational	Destroy, Disrupt, Delay	Usability	Joint Operation Planning and Execution System (JOPES)/ Targeting Process	Individuals, Governments, Militaries
	Electronic Protection	Physical	Protect the Use of Electro-magnetic Spectrum	Security	JOPES/Defense Planning	Individuals, Businesses, Governments, Militaries
	Electronic Warfare Support	Physical	Identify and Locate Threats	Usability	Joint Intelligence Preparation of the Battlespace(JIPB)/SIGINT Collection	Militaries
Computer Network Operations	Computer Network Attack	Physical, Informational	Destroy, Disrupt, Delay	Security	JIPB/JOPES/Targeting Process	Individuals, Governments, Militaries
	Computer Network Defense	Physical, Informational	Protect Computer Networks	Security	JOPES/J-6 Vulnerability Analysis	Individuals, Businesses, Governments, Militaries
	Computer Network Exploitation	Informational	Gain Information From and About Computers and Computer Networks	Security	JIPB/Targeting Process	Individuals, Governments, Militaries
Psychological Operations	Psychological Operations	Cognitive	Influence	Relevance	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Military Deception	Military Deception	Cognitive	Mislead	Accuracy	JOPES/Joint Operation Planning	Militaries
Operations Security	Operations Security	Cognitive	Deny	Security	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Supporting Capabilities	Information Assurance	Informational	Protect Information and Informatin Systems	Security	JOPES/J-6 Vulnerability Analysis	Businesses, Governments, Militaries
	Physical Security	Physical	Secure Information and Information Infrastructure	Usability	JOPES/Defense Planning	Businesses, Governments, Militaries
	Physical Attack	Physical	Destroy, Disrupt	Usability	JOPES/Joint Operation Planning	Governments, Militaries
	Counterintelligence	Cognitive	Mislead	Accuracy	JIPB/Human Intelligence Collection	Governments, Militaries
	Combat Camera	Physical	Inform/Document	Usability, Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
Related Capabilities	Civil Military Operations	Cognitive	Influence	Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
	Public Affairs	Cognitive	Inform	Accuracy	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
	Public Diplomacy	Cognitive	Inform	Accuracy	Interagency Coordination	Governments

Figure I-3. Information Operations Integration into Joint Operations (Notional)

c. **IO's ability to affect and defend decision making is based on five fundamental assumptions.** Although each of these assumptions is an important enabling factor for IO, they will not all necessarily be true for every operation. For any specific operation where one or more of these assumptions are not met, the risk assessment provided to the commander would be adjusted accordingly.

(1) Generally, the quality of information that is considered valuable to human and automated decision makers is universal. However, the relative importance of each quality criterion of information (Figure I-2) may vary based on the influences of geography, language, culture, religion, organization, experience, or personality.

(2) Decisions are made based on the information available at the time.

(3) It is possible, with finite resources, to understand the relevant aspects of the information environment to include the processes decision makers use to make decisions.

(4) It is possible to affect the information environment in which specific decision makers act through psychological, electronic, or physical means.

(5) It is possible to measure the effectiveness of IO actions in relation to an operational objective.

d. Since human activity takes place in the information environment, it is potentially subject to IO. However, **only mission-related critical psychological, electronic, and physical points in the information environment should be targeted, directly or indirectly, by IO**. The planning methodologies used to identify and prioritize such points in planning IO are discussed in Chapter V, "Planning and Coordination."

e. **IO capabilities can produce effects and achieve objectives at all levels of war and across the range of military operations**. The nature of the modern information environment complicates the identification of the boundaries between these levels. Therefore, **at all levels, information activities, including IO must be consistent with broader national security policy and strategic objectives**.

f. **Because IO are conducted across the range of military operations,** and can make significant contributions before major operations commence, the IO environment should be prepared and assessed through a variety of engagement and intelligence activities, all designed to make IO more effective. In addition to impacting the environment prior to the onset of military operations, IO are essential to post-combat operations. Therefore, integration, planning, employment, and assessment of core, supporting, and related IO are vital to ensuring a rapid transition to a peaceful environment.

g. **The ultimate strategic objective of IO is to deter a potential or actual adversary or other TA from taking actions that threaten US national interests**. Additionally, IO actions executed through civilian controlled portions of the global information environment, or which may cause unintended reactions from US or foreign populaces, must account for US policy and

legal issues, as well as potentially disruptive infrastructure issues, through civil-military coordination at all levels.

(1) **IO may target human decision making or automated decision support systems with specific actions**. Technology allows automated decision making to be targeted with increasing precision and affords more sophisticated ways to protect it. However, **targeting automated decision making, at any level, is only as effective as the human adversary's reliance on such decisions**.

(2) The focus of IO is on the decision maker and the information environment in order to affect decision making and thinking processes, knowledge, and understanding of the situation. **IO can affect data, information, and knowledge in three basic ways**:

(a) By taking specific psychological, electronic, or physical actions that add, modify, or remove information from the environment of various individuals or groups of decision makers.

(b) By taking actions to affect the infrastructure that collects, communicates, processes, and/or stores information in support of targeted decision makers.

(c) By influencing the way people receive, process, interpret, and use data, information, and knowledge.

h. **All IO capabilities may be employed in both offensive and defensive operations.** Commanders use IO capabilities in both offensive and defensive operations simultaneously to accomplish the mission, increase their force effectiveness, and protect their organizations and systems. Fully integrating IO capabilities for offensive and defensive operations requires planners to treat IO as a single function. Commanders can use IO capabilities to accomplish the following:

(1) **Destroy.** To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.

(2) **Disrupt.** To break or interrupt the flow of information.

(3) **Degrade.** To reduce the effectiveness or efficiency of adversary C2 or communications systems, and information collection efforts or means. IO can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.

(4) **Deny.** To prevent the adversary from accessing and using critical information, systems, and services.

(5) **Deceive.** To cause a person to believe what is not true. MILDEC seeks to mislead adversary decision makers by manipulating their perception of reality.

(6) **Exploit.** To gain access to adversary C2 systems to collect information or to plant false or misleading information.

(7) **Influence.** To cause others to behave in a manner favorable to US forces.

(8) **Protect.** To take action to guard against espionage or capture of sensitive equipment and information.

(9) **Detect.** To discover or discern the existence, presence, or fact of an intrusion into information systems.

(10) **Restore.** To bring information and information systems back to their original state.

(11) **Respond.** To react quickly to an adversary's or others' IO attack or intrusion.

5. Strategic Communication

a. Strategic Communication constitutes focused USG efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power.

b. DOD efforts must be part of a government-wide approach to develop and implement a more robust strategic communication capability. DOD must also support and participate in USG strategic communication activities to understand, inform, and influence relevant foreign audiences to include: DOD's transition to and from hostilities, security, military forward presence, and stability operations. This is primarily accomplished through its PA, DSPD, and IO capabilities.

c. DOD PA, DSPD, and IO are distinct functions that can support strategic communication. Synchronization of strategic communication-related PA, IO, and DSPD activities is essential for effective strategic communication.

d. Combatant commanders should ensure planning for IO, PA, and DSPD are consistent with overall USG strategic communication objectives and are approved by the Office of the Secretary of Defense (OSD). Combatant commanders should integrate an information strategy into planning for peacetime and contingency situations. Combatant commanders plan, execute, and assess PA, DSPD, and IO activities to implement theater security cooperation plans (TSCPs), to support US embassies' information programs, and to support other agencies' public diplomacy and PA programs directly supporting DOD missions.

6. Importance of Information Operations in Military Operations

a. History indicates that the speed and accuracy of information available to military commanders is the significant factor in determining the outcome on the battlefield. IO enables

the accuracy and timeliness of information required by US military commanders by defending our systems from exploitation by adversaries. IO are used to deny adversaries access to their C2 information and other supporting automated infrastructures.

b. Adversaries are increasingly exploring and testing IO actions as asymmetric warfare that can be used to thwart US military objectives that are heavily reliant on information systems. This requires the US military to employ defensive technologies and utilize leading-edge tactics and procedures to prevent our forces and systems from being successfully attacked.

Intentionally Blank

CHAPTER II
CORE, SUPPORTING, AND RELATED INFORMATION OPERATIONS CAPABILITIES

"The instruments of battle are valuable only if one knows how to use them."

Charles Ardant du Picq 1821 - 1870

1. Introduction

IO coordinates and synchronizes the employment of the five core capabilities in support of the combatant commander's objectives or to prevent the adversary from achieving his desired objectives. The core capabilities are: PSYOP, MILDEC, OPSEC, EW, and CNO. There are five supporting capabilities: IA, physical security, physical attack, CI, and COMCAM, and three related capabilities: PA, CMO, and DSPD. Together these capabilities enable the commander to affect and influence a situation. However, the potential for conflict between interrelated capabilities requires their employment be coordinated, integrated, and synchronized.

2. Core Information Operations Capabilities

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

b. **Psychological Operations**

(1) PSYOP are planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. PSYOP are a vital part of the broad range of US activities to influence foreign audiences and are the only DOD operations authorized to influence foreign TAs directly through the use of radio, print, and other media. PSYOP personnel advise the supported commander on methods to capitalize on the psychological impacts of every aspect of force employment, and how to develop a strategy for developing and planning the dissemination of specific PSYOP programs, to achieve the overall campaign objectives. During a crisis, a PSYOP assessment team (POAT) deploys at the request of the supported commander. A POAT is a small, tailored team of PSYOP planners, product distribution/dissemination, and logistics specialists. The POAT assesses the situation, develops PSYOP objectives, and recommends the appropriate level of support to accomplish the mission. A POAT can augment a unified command or Joint Task Force (JTF) staff and provide PSYOP planning support. The senior PSYOP officer in the operational area, normally the joint psychological operations task force (JPOTF) commander, may also serve as the de facto joint force PSYOP officer. Working through the various component operations staffs, the joint

force PSYOP officer ensures continuity of psychological objectives and identifies themes to stress and avoid.

(2) **PSYOP as an IO Core Capability.** PSYOP has a central role in the achievement of IO objectives in support of the JFC. In today's information environment even PSYOP conducted at the tactical level can have strategic effects. Therefore, PSYOP has an approval process that must be understood and the necessity for timely decisions is fundamental to effective PSYOP and IO. This is particularly important in the early stages of an operation given the time it takes to develop, design, produce, distribute, disseminate, and evaluate PSYOP products and actions. All PSYOP are conducted under the authority of interagency-coordinated and OSD approved PSYOP programs. The PSYOP program approval process at the national level requires time for sufficient coordination and resolution of issues; hence, JFCs should begin PSYOP planning as early as possible to ensure the execution of PSYOP in support of operations. A JFC must have an approved PSYOP program, execution authority, and delegation of product approval authority before PSYOP execution can begin. JFCs should request PSYOP planners immediately during the initial crisis stages to ensure the JFC has plenty of lead time to obtain the proper authority to execute PSYOP. PSYOP assets may be of particular value to the JFC in pre-/post-combat operations when other means of influence are restrained or not authorized. PSYOP must be coordinated with CI, MILDEC, and OPSEC to ensure deconfliction and control, CI operations are not compromised, and that all capabilities within IO are coordinated to achieve the objectives established in planning. There must be close cooperation and coordination between PSYOP and PA staffs in order to maintain credibility with their respective audiences, which is the purpose of the IO cell. PSYOP efforts are most effective when personnel with a thorough understanding of the language and culture of the TA are included in the review of PSYOP materials and messages. As the information environment evolves, the dissemination of PSYOP products is expanding from traditional print and broadcast to more sophisticated use of the Internet, facsimile messaging, text messaging, and other emerging media. The effectiveness of PSYOP is enhanced by the synchronization and coordination of the core, supporting, and related capabilities of IO; particularly PA, MILDEC, CNO, CMO, and EW.

For more discussion on PSYOP, see Joint Publication (JP) 3-53, Joint Doctrine for Psychological Operations.

c. **Military Deception**

(1) MILDEC is described as being those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces' mission. MILDEC and OPSEC are complementary activities — MILDEC seeks to encourage incorrect analysis, causing the adversary to arrive at specific false deductions, while OPSEC seeks to deny real information to an adversary, and prevent correct deduction of friendly plans. To be effective, a MILDEC operation must be susceptible to adversary collection systems and "seen" as credible to the enemy commander and staff. A plausible approach to MILDEC planning is to employ a friendly course of action (COA) that can be executed by friendly forces and that adversary intelligence can verify. However, MILDEC planners must not fall into the trap of ascribing to the adversary particular attitudes, values, and reactions that "mirror image" likely friendly actions in the same situation, i.e., assuming that the adversary will respond or act in a particular manner based on how we would respond. There are

always competing priorities for the resources required for deception and the resources required for the real operation. For this reason, the deception plan should be developed concurrently with the real plan, starting with the commander's and staff's initial estimate, to ensure proper resourcing of both. To encourage incorrect analysis by the adversary, it is usually more efficient and effective to provide a false purpose for real activity than to create false activity. OPSEC of the deception plan is at least as important as OPSEC of the real plan, since compromise of the deception may expose the real plan. This requirement for close hold planning while ensuring detailed coordination is the greatest challenge to MILDEC planners. On joint staffs, MILDEC planning and oversight responsibility is normally organized as a staff deception element in the operations directorate of a joint staff (J-3).

(2) **MILDEC as an IO Core Capability.** MILDEC is fundamental to successful IO. It exploits the adversary's information systems, processes, and capabilities. MILDEC relies upon understanding how the adversary commander and supporting staff think and plan and how both use information management to support their efforts. This requires a high degree of coordination with all elements of friendly forces' activities in the information environment as well as with physical activities. Each of the core, supporting, and related capabilities has a part to play in the development of successful MILDEC and in maintaining its credibility over time. While PA should not be involved in the provision of false information, it must be aware of the intent and purpose of MILDEC in order not to inadvertently compromise it.

For more discussion on MILDEC, see JP 3-58, Joint Doctrine for Military Deception.

d. **Operations Security**

(1) OPSEC is a process of identifying critical information and subsequently analyzing friendly actions and other activities to: identify what friendly information is necessary for the adversary to have sufficiently accurate knowledge of friendly forces and intentions; deny adversary decision makers critical information about friendly forces and intentions; and cause adversary decision makers to misjudge the relevance of known critical friendly information because other information about friendly forces and intentions remain secure. On joint staffs, responsibilities for OPSEC are normally delegated to the J-3. A designated OPSEC program manager supervises other members of the command-assigned OPSEC duties and oversees the coordination, development, and implementation of OPSEC as an integrated part of IO in the operational area.

(2) **OPSEC as an IO Core Capability.** OPSEC denies the adversary the information needed to correctly assess friendly capabilities and intentions. In particular, OPSEC complements MILDEC by denying an adversary information required to both assess a real plan and to disprove a deception plan. For those IO capabilities that exploit new opportunities and vulnerabilities, such as EW and CNO, OPSEC is essential to ensure friendly capabilities are not compromised. The process of identifying essential elements of friendly information and taking measures to mask them from disclosure to adversaries is only one part of a defense-in-depth approach to securing friendly information. To be effective, other types of security must complement OPSEC. Examples of other types of security include physical security, IA programs, computer network defense (CND), and personnel programs that screen personnel and limit authorized access.

For more discussion on OPSEC, see JP 3-54, Operations Security.

e. **Electronic Warfare**

(1) EW refers to any military action involving the use of electromagnetic (EM) and directed energy to control the EM spectrum or to attack the adversary. EW includes three major subdivisions: EA, electronic protection (EP), and electronic warfare support (ES). EA involves the use of EM energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying adversary combat capability. EP ensures the friendly use of the EM spectrum. ES consists of actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. ES provides information required for decisions involving EW operations and other tactical actions such as threat avoidance, targeting, and homing. ES data can be used to produce SIGINT, provide targeting for electronic or other forms of attack, and produce measurement and signature intelligence (MASINT). SIGINT and MASINT can also provide battle damage assessment (BDA) and feedback on the effectiveness of the overall operational plan.

(2) **EW as an IO Core Capability.** EW contributes to the success of IO by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EM spectrum while protecting friendly freedom of action in that spectrum. Expanding reliance on the EM spectrum for informational purposes increases both the potential and the challenges of EW in IO. The increasing prevalence of wireless telephone and computer usage extends both the utility and threat of EW, offering opportunities to exploit an adversary's electronic vulnerabilities and a requirement to identify and protect our own from similar exploitation. As the use of the EM spectrum has become universal in military operations, so has EW become involved in all aspects of IO. All of the core, supporting, and related IO capabilities either directly use EW or indirectly benefit from EW. In order to coordinate and deconflict EW, and more broadly all military usage of the EM spectrum, an electronic warfare coordination cell (EWCC) should be established by the JFC to reside with the component commander most appropriate to the operation. In addition, all joint operations require a joint restricted frequency list (JRFL). This list specifies protected, guarded, and taboo frequencies that should not normally be disrupted without prior coordination and planning, either because of friendly use or friendly exploitation. This is maintained and promulgated by the communications system directorate of a joint staff (J-6) in coordination with J-3 and the joint commander's electronic warfare staff (or EWCC, if delegated).

For more discussion on EW, see JP 3-51, Joint Doctrine for Electronic Warfare.

f. **Computer Network Operations**

(1) CNO is one of the latest capabilities developed in support of military operations. CNO stems from the increasing use of networked computers and supporting IT infrastructure systems by military and civilian organizations. CNO, along with EW, is used to attack, deceive, degrade, disrupt,

deny, exploit, and defend electronic information and infrastructure. For the purpose of military operations, CNO are divided into CNA, CND, and related computer network exploitation (CNE) enabling operations. CNA consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. CND actions not only protect DOD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations. CNE is enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Note that due to the continued expansion of wireless networking and the integration of computers and radio frequency communications, there will be operations and capabilities that blur the line between CNO and EW and that may require case-by-case determination when EW and CNO are assigned separate release authorities.

(2) **CNO as an IO Core Capability.** The increasing reliance of unsophisticated militaries and terrorist groups on computers and computer networks to pass information to C2 forces reinforces the importance of CNO in IO plans and activities. As the capability of computers and the range of their employment broadens, new vulnerabilities and opportunities will continue to develop. This offers both opportunities to attack and exploit an adversary's computer system weaknesses and a requirement to identify and protect our own from similar attack or exploitation.

The doctrinal use of CNO capabilities in support of IO is discussed further in Appendix A, "Supplemental Guidance," to this publication.

g. **Mutual Support Among IO Capabilities.** A more detailed description of how the IO core capabilities mutually support one another is illustrated in the table at Appendix B, "Mutual Support Between Information Operations Core Capabilities." This shows some of the positive interrelationships between the contributors to IO effects. For each positive contribution, there is also the possibility of negative effects if these capabilities, which all operate in the information environment, are not fully coordinated. The development of effective IO across the range of military operations depends upon a full understanding of this interrelationship among capabilities. Only then can they be properly and effectively integrated through the processes discussed in Chapter V, "Planning and Coordination."

3. Information Operations Supporting Capabilities

a. Capabilities supporting IO include IA, physical security, physical attack, CI, and COMCAM. These are either directly or indirectly involved in the information environment and contribute to effective IO. They should be integrated and coordinated with the core capabilities, but also serve other wider purposes.

b. **Information Assurance**

(1) IA is defined as measures 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. IA is necessary to gain and maintain information superiority. IA requires a defense-in-depth approach that integrates the capabilities of people, operations, and technology to establish multilayer and multidimensional protection to ensure survivability and mission accomplishment. IA must assume that access can be gained to information and information systems from inside and outside DOD-controlled networks. In joint organizations, IA is a responsibility of the J-6.

(2) **IA as a Supporting Capability for IO.** IO depends on IA to protect information and information systems, thereby assuring continuous capability. IA and IO have an operational relationship in which IO are concerned with the coordination of military activities in the information environment, while IA protects the electronic and automated portions of the information environment. IA and all aspects of CNO are interrelated and rely upon each other to be effective. IO relies on IA to protect infrastructure to ensure its availability to position information for influence purposes and for the delivery of information to the adversary. Conversely, IA relies on IO to provide operational protection with coordinated OPSEC, EP, CND, and CI against adversary IO or intelligence efforts directed against friendly electronic information or information systems.

For detailed policy guidance, see DOD Directive (DODD) 8500.1, Information Assurance (IA)*, DOD Instruction (DODI) 8500.2,* Information Assurance (IA) Implementation. *Joint policy is established in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3401.03,* Information Assurance (IA) and Computer Network Defense (CND) Joint Quarterly Readiness Review (JQRR) Metrics*, and CJCSI 6510.01 Series,* Information Assurance (IA) and Computer Network Defense (CND).

c. **Physical Security**

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

(2) **Physical Security as a Supporting Capability for IO.** Just as IA protects friendly electronic information and information systems, physical security protects physical facilities containing information and information systems worldwide. Physical security often contributes to OPSEC, particularly in the case of MILDEC, when compromise of the MILDEC activity could compromise the real plan. IO plans may require significant physical security resources and this requirement should be made clear to the J-3 as early as possible in the planning process.

For more discussion on physical security, see JP 3-07.2, Antiterrorism*, JP 3-57,* Joint Doctrine for Civil-Military Operations*, and in general, JP 3-10,* Joint Security Operations in Theater.

d. **Physical Attack**

(1) The concept of attack is fundamental to military operations. Physical attack disrupts, damages, or destroys adversary targets through destructive power. Physical attack can also be used to create or alter adversary perceptions or drive an adversary to use certain exploitable information systems.

(2) **Physical Attack as a Supporting Capability for IO.** Physical attack can be employed in support of IO as a means of attacking C2 nodes to affect enemy ability to exercise C2 and of influencing TAs. IO capabilities, for example PSYOP, can be employed in support of physical attack to maximize the effect of the attack on the morale of an adversary. The integration and synchronization of fires with IO through the targeting process is fundamental to creating the necessary synergy between IO and more traditional maneuver and strike operations. In order to achieve this integration, commanders must be able to define the effects they seek to achieve and staffs will incorporate these capabilities into the commander's plan. Specifically, due to the fast-paced conduct of air operations, it is crucial that the planning and execution of both IO and air operations be conducted concurrently to produce the most effective targeting plan. Considerations of targeting are discussed in more detail in Chapter V, "Planning and Coordination."

e. **Counterintelligence**

(1) CI consists of 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, foreign persons, or international terrorist activities. The CI programs in joint staffs are a responsibility of the CI and human intelligence staff element of the intelligence directorate.

(2) **CI as a Supporting Capability for IO.** CI procedures are a critical part of guarding friendly information and information systems. A robust security program that integrates IA, physical security, CI, and OPSEC with risk management procedures offers the best chance to protect friendly information and information systems from adversary actions. CNO provide some of the tools needed to conduct CI operations. For the IO planner, CI analysis offers a view of the adversary's information-gathering methodology. From this, CI can develop the initial intelligence target opportunities that provide access to the adversary for MILDEC information, PSYOP products, and CNA/CNE actions.

For more discussion on CI, see classified JP 2-01.2, Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations.

f. **Combat Camera**

(1) The COMCAM mission is to provide the OSD, the Chairman of the Joint Chiefs of Staff (CJCS), the Military Departments, the combatant commands, and the JTF with an imagery capability in support of operational and planning requirements across the range of military operations. COMCAM is responsible for rapid development and dissemination of products that support strategic and operational

IO objectives. The COMCAM program belongs to the Defense Visual Information Directorate, which falls under the Assistant Secretary of Defense for Public Affairs. When deployed, operational control of COMCAM forces can be delegated to any echelon of command at the discretion of the JFC and subordinate commanders. COMCAM may be coordinated by the IO staff at the JFC, component, and subordinate unit levels. Most large JTF organizations will have a joint COMCAM management team assigned to manage COMCAM, and to assist in the movement of imagery. Additionally, there are usually one or more joint or component specific COMCAM teams assigned to the theater. These component teams may be assigned to special operations forces (SOF) or other specific units.

(2) **Combat Camera as a Supporting Capability for IO.** COMCAM supports all of the capabilities of IO that use images of US or friendly force operations, whether to influence an adversary or other TAs or support US forces or allies. They provide images for PSYOP, MILDEC, PA, and CMO use, but can also be used for BDA/measures of effectiveness (MOEs) analysis. COMCAM can also provide records of IO actions for subsequent rebuttal proceedings. However, COMCAM imagery must be controlled in order to ensure that OPSEC is maintained and valuable information is not released to the adversary. The quality and format, including digital video/still photography, night and thermal imagery, means that COMCAM products can be provided to professional news organizations by PA when they are unable to provide their own imagery.

For more discussion on COMCAM, see Multi-Service Tactics, Techniques, and Procedures for Joint Combat Camera *of March 2003*.

4. Information Operations Related Capabilities

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

b. **Public Affairs**

(1) PA are those public information, command information, and community relations activities directed toward both external and internal audiences with interest in DOD. PA is essential for joint forces information superiority, and credible PA operations are necessary to support the commander's mission and maintain essential public liaisons. PA's principal focus is to inform domestic and international audiences of joint operations to support combatant command public information needs (see Figure II-1).

(2) **PA as a Related Capability to IO.** PA and IO must be coordinated and synchronized to ensure consistent themes and messages are communicated to avoid credibility losses. As with other related IO capabilities, PA has a role in all aspects of DOD's missions and functions. Communication of operational matters to internal and external audiences is just one part of PA's function. In performing

duties as one of the primary spokesmen, the public affairs officer's interaction with the IO staff enables PA activities to be integrated, coordinated, and deconflicted with IO. While intents differ, PA and IO ultimately support the dissemination of information, themes, and messages adapted to their audiences. PA contributes to the achievement of military objectives, for instance, by countering adversary misinformation and disinformation through the publication of accurate information. PA also assists OPSEC by ensuring that the media are aware of the implications of premature release of information. The embedding of media in combat units offers new opportunities, as well as risks, for the media and the military; the PA staff has a key role in establishing embedding ground rules. Many adversaries rely on limiting their population's knowledge to remain in power; PA and IO provide ways to get the joint forces' messages to these populations.

For more discussion on PA, see JP 3-61, Public Affairs.

c. **Civil-Military Operations**

(1) CMO are the activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace. They are conducted across the range of military operations to address root causes of instability, assist in reconstruction after conflict or disaster, or may be conducted independent of other military operations to support US national security objectives. CMO can occur in friendly, neutral, or hostile operational areas to facilitate military operations and achieve US objectives.

PRINCIPLES OF PUBLIC INFORMATION

- **Information shall be made fully and readily available, consistent with statutory requirements, unless its release is precluded by national security constraints or valid statutory mandates or exceptions. The "Freedom of Information Act" shall be supported in both letter and spirit.**
- **A free flow of general and military information shall be made available, without censorship or propaganda, to the men and women of the Armed Forces and their dependents.**
- **Information shall not be classified or otherwise withheld to protect the Government from criticism or embarrassment.**
- **Information shall be withheld only when disclosure would adversely affect national security, or threaten the safety or privacy of the men and women of the Armed Forces.**
- **The Department of Defense's (DOD's) obligation to provide the public with information on DOD major programs may require detailed public affairs planning and coordination in the DOD and with other Government Agencies. Such activity is to expedite the flow of information to the public.**

Figure II-1. Principles of Public Information

CMO may include performance by military forces of activities and functions that are normally the responsibility of local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. CMO may be performed by designated civil affairs (CA), by other military forces, or by a combination of CA and other forces. Certain types of organizations are particularly suited to this mission and form the nucleus of CMO. These units are typically CA and PSYOP units. Others, such as, but not limited to, other SOF, engineers, health service support, transportation, military police and security forces, may act as enablers. Personnel skilled in the language and culture of the population are essential to CMO.

(2) **CMO as a Related Capability to IO.** CMO can be particularly effective in peacetime and pre-/post-combat operations when other capabilities and actions may be constrained. Early consideration of the civil-military environment in which operations will take place is important. As with PA, the CMO staff also has an important role to play in the development of broader IO plans and objectives. As the accessibility of information to the widest public audiences increases and as military operations increasingly are conducted in open environments, the importance of CMO to the achievement of IO objectives will increase. At the same time the direct involvement of CMO with core, supporting and related IO capabilities (for instance PSYOP, CNO, and CI) will also increase. CMO, by their nature, usually affect public perceptions in their immediate locale. Distribution of information about CMO efforts and results through PA and PSYOP can affect the perceptions of a broader audience and favorably influence key groups or individuals.

For more discussion on CMO, see JP 3-57, Joint Doctrine for Civil-Military Operations.

d. **Defense Support to Public Diplomacy**

(1) DSPD consists of activities and measures taken by DOD components, not solely in the area of IO, to support and facilitate public diplomacy efforts of the USG.

(2) **DSPD, PD, and IO.** DOD contributes to PD, which includes those overt international information activities of the USG designed to promote US foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers and by broadening the dialogue between American citizens and institutions and their counterparts abroad. When approved, PSYOP assets may be employed in support of DSPD as part of security cooperation initiatives or in support of US embassy PD programs. Much of the operational level IO activity conducted in any theater will be directly linked to PD objectives. DSPD requires coordination with both the interagency and among DOD components.

For more discussion on DSPD, see DODD 3600.1, Information Operations (IO).

CHAPTER III
INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS

"To understand human decisions and human behavior requires something more than an appreciation of immediate stimuli. It requires, too, a consideration of the totality of forces, material and spiritual, which condition, influence or direct human responses. And because we are dealing with human beings, the forces which helped shape their actions must be recognized as multiple, subtle, and infinitely complex."

David Herlihy, *The History of Feudalism*

1. Introduction

Like all other aspects of joint operations, IO requires effective intelligence support. IO is intelligence intensive in particular and therefore successful planning, preparation, execution, and assessment of IO demand detailed and timely intelligence. This chapter briefly discusses how intelligence supports the planning and execution of IO.

2. Intelligence Support to Information Operations

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

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

(1) **Physical Properties of the Information Environment.** Physical properties of the information environment include people, places, things, and capabilities of information infrastructure and adversary information capabilities. Examples include:

(a) Geographic coordinates of adversary information infrastructure and capabilities.

(b) Organization of infrastructure and capabilities as well as identification of critical links, nodes, and redundant communication infrastructure.

(c) Types, quantity, and configuration of information infrastructure and capabilities (with specific makes, models, and numbers).

(d) Organizational planning, decision, and execution processes.

(e) Enemy intelligence/feedback mechanism for gaining battlespace awareness, information, and knowledge.

(f) Enemy computer attack, defense, and exploitation capabilities.

(2) **Informational Properties of the Information Environment.** Informational properties of the information environment include those systems and networks where information is created, processed, manipulated, transmitted, and shared. It includes those properties relevant to the electronic collection, transmission, processing, storage, and display of information. These properties may be electronic or human-to-human or a combination of both. They describe the formal and informal communications infrastructure and networks, kinship and descent relationships, licit and illicit commercial relationships and social affiliations and contacts that collectively create, process, manipulate, transmit, and share information in an operational area and among TAs. Examples of informational properties include:

(a) Specification, capacity, configuration, and usage of information infrastructure and capabilities.

(b) Technical design of information infrastructure.

(c) Networks of human-to-human contact used for the transmission of information (couriers, rat-lines, dead-drops, etc.).

(d) Social and commercial networks that process and share information and influence (kinship and descent linkages, formal and informal social contacts, licit and illicit commercial affiliations and records of ownership and transactions, etc.).

(e) Content and context.

(3) **Cognitive Properties of the Information Environment.** Cognitive properties of the information environment are the psychological, cultural, behavioral, and other human attributes that influence decision making, the flow of information, and the interpretation of information by individuals or groups at any level in a state or organization. Cognitive properties may include:

(a) Cultural and societal factors affecting attitudes and perceptions such as language, education, history, religion, myths, personal experience, and family structure.

(b) Identity of key individuals and groups affecting attitudes and perceptions, whether in the same or a different country as those they influence.

(c) Identity and psychological profile of key decision makers, their advisors, key associates, and/or family members who influence them.

(d) Credibility of key individuals or groups and specification of their sphere of influence.

(e) Laws, regulations, and procedures relevant to information and decision making, decision-making processes, capability employment doctrine, timeliness, and information content.

(f) How leaders think, perceive, plan, execute, and assess outcomes of their results and actions from their perspectives.

(g) Identify key historical events between the target country and the US, which may affect an individual or group's attitudes and perceptions of the US, whether in the same or different country as those they influence.

(4) While these broad types of properties of the information environment illustrate the diversity of IO intelligence requirements, it is important to note that multiple sources and methods may be required to collect physical, informational, and cognitive properties of specific collection targets in order to fuse and analyze different properties in support of IO planning. For instance, if operational planning requires intelligence on radio stations within an adversary country, that requirement may include the number and location of broadcast and transmission facilities (physical), the technical specifications of each station (informational), the identity of owners and key personnel, and the credibility or popularity of each station (cognitive).

b. **Intelligence Support to IO Planning.** Intelligence support is an integral part of IO planning. In particular, the joint intelligence preparation of the battlespace (JIPB) process provides a valuable methodology for identifying capabilities, vulnerabilities, and critical nodes within the information environment. JP 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*, discusses JIPB support to IO. A sequential overview of intelligence support to IO planning includes actions to:

(1) Identify adversary information value, use, flow, and vulnerabilities relevant to specific types of decision making.

(2) Identify individual systems and target sets relevant to specified adversary or other TA decision making.

(3) Identify desired effects appropriate to individual systems and target sets.

(4) Predict the consequences (non-objective related outcomes) of identified actions.

(5) Coordinate with planning personnel to establish priority of intelligence requirements.

(6) Assist in developing IO assessment criteria during planning and then assist in monitoring and assessing IO during execution (which may extend before and after execution of conventional operations).

(7) Tailor assessment/feedback methodologies to specific operations.

(8) Evaluate the outcome of executed IO activities/tasks.

(9) Provide assessment for IO actions relative to JFC objectives and mission.

c. **Intelligence Considerations in Planning Information Operations**

(1) **Information Environment Impact on Intelligence Support.** The nature of the information environment has profound implications for intelligence support to IO. Members of the operational community and the intelligence community must understand these implications in order to efficiently request and provide quality intelligence support to IO. These implications are listed below.

(a) **Intelligence Resources are Limited.** Information collection requirements are almost limitless, especially for many types of IO. Commanders and their intelligence and operations directorates must work together to identify IO intelligence requirements and ensure that they are given high enough priority in the commander's requests to the intelligence community (IC).

(b) **Collection Activities are Legally Constrained.** The nature of the information environment complicates compliance with legal constraints and restraints. Thus the IC must implement technical and procedural methods to ensure compliance with the law. Additionally, intelligence may be supplemented with information legally provided by law enforcement or other sources. Especially in the area of CNO, where the application of different domestic and international laws may be unclear, close coordination among the operational, legal, and law enforcement communities is essential.

(c) **IO Intelligence Often Requires Long Lead Times.** The intelligence necessary to affect adversary or other TA decisions often requires that specific sources and methods be positioned and employed over time to collect the necessary information and conduct analyses required for IO planning. Commanders and their staffs, including IO planners, must be aware of the relative lead times required to develop different types of intelligence both for initial planning and for feedback during operations. To deal with these long lead times, the commander must provide detailed initial guidance to the staff during the mission analysis and estimate processes.

(d) **The Information Environment is Dynamic.** The information environment changes over time according to different factors. Physical changes may occur more slowly and may be easier to detect than informational or cognitive changes. Commanders and their staffs must understand both the timeliness of the intelligence they receive and the differing potentials for change in the dimensions of the information environment. The implication is that we must have agile intellects, intelligence systems, and organizational processes to exploit this dynamic environment.

(e) **Properties of the Information Environment Affect Intelligence.** Collection of physical and electronic information is objectively measurable by location and quantity. While

identification of key individuals and groups of interest may be a relatively straightforward challenge, the relative importance of various individuals and groups, their psychological profiles, and how they interact is not easily agreed upon nor quantified. Commanders and their staffs must have an appreciation for the subjective nature of psychological profiles and human nature. They must also continue to pursue effective means of trying to measure subjective elements using MOEs and other applicable techniques.

(2) **Coordination of Planned IO with Intelligence.** Coordination should occur among intelligence, targeting, IO, and collection management personnel. The requirement for accurate intelligence gain/loss and political/military assessments, when determining targets to attack and means of employment, is central to the integration of IO.

(3) **Foreign Perceptions and Human Factors Analysis.** Assessing foreign perceptions is necessary for successful IO activities. Preparing the modern battlespace for successful joint operations relies on a thorough understanding of the information environment, including foreign perceptions, TA analysis, and cultural analysis. Geographic combatant commanders require IC support to continually assess foreign perceptions of support for the areas of responsibility (AORs) TSCP efforts, along with Joint Operation Planning and Execution System (JOPES) planning activities. Human factors analysis in conjunction with an understanding of the cultural environment are also important in avoiding projection of US cultural bias on TAs (mirror imaging). Intelligence resources contribute to assessing of foreign populations through human factors analysis, influence net modeling, foreign media analysis, media mapping, polling/focus group analysis, and key communicators/sources of influence analysis. This is, for the most part, open source intelligence and must be interpreted and synthesized by country/cultural intelligence subject matter experts (SMEs).

(4) **Priority of Effort.** The requirement to collect, analyze, and produce detailed intelligence of the granularity required for IO currently exceeds the resources of the IC. Assigning intelligence resources to IO as with all operations is regulated based on established requirements and processes within the IC. It is imperative that intelligence requirements be coordinated and prioritized at each level of command.

d. **Sources of Intelligence Support**

(1) Through the intelligence directorate of a joint staff (J-2), **IO planners and supporting joint organizations have access to intelligence** from the national and combatant command-level intelligence producers and collectors. **At the combatant command level**, the theater joint intelligence center supports IO planning and execution and provides support to JTFs through established joint intelligence support elements. In **multinational operations**, when appropriate, the J-2 should share information and assessments with allies and coalition partners.

(2) The J-2 on each joint staff normally assigns specific J-2 personnel to coordinate with IO planners and capability specialties through the IO cell or other IO staff organizations established by the JFC.

Intentionally Blank

CHAPTER IV
RESPONSIBILITIES AND COMMAND RELATIONSHIPS

"Good will can make any organization work; conversely the best organization in the world is unsound if the men who have to make it work don't believe in it."

James Forrestal

1. Introduction

This chapter describes the JFC's authority for IO, specific responsibilities established in DODD 3600.1, *Information Operations (IO)*, and the *Unified Command Plan*, command relationships between the DOD components responsible for IO, the organization of combatant command and JTF staffs for IO, and joint boards, processes, and products related to IO.

2. Authorities and Responsibilities

a. **Authorities.** IO in one combatant command AOR may affect other AORs directly or indirectly. To address this complication, the President has given Commander, United States Strategic Command (CDRUSSTRATCOM) specific responsibility to coordinate IO (core capabilities) across combatant command AOR boundaries.

b. **Responsibilities**

(1) Responsibilities for IO are established in DODD 3600.1, *Information Operations (IO)*. The commanders of the combatant commands shall integrate, plan, execute, and assess IO when conducting campaigns across the range of military operations and shall identify and prioritize IO requirements. IO shall be integrated into appropriate security cooperation plans and activities.

(2) In accordance with change 2 to Unified Command Plan for Fiscal Year '04 CDRUSSTRATCOM integrates and coordinates DOD IO that cross AOR boundaries including:

(a) Supporting other combatant commanders for planning.

(b) Planning and coordinating capabilities that have trans-regional effects or that directly support national objectives.

(c) Exercising C2 of selected missions if directed to do so by the President or the Secretary of Defense (SecDef).

(d) Planning, directing, and identifying desired characteristics and capabilities for DOD-wide CND.

(e) Identifying desired characteristics and capabilities of CNA, conducting CNA in support of assigned missions, and integrating CNA capabilities in support of other combatant commanders, as directed.

(f) Identifying desired characteristics and capabilities for joint EW and planning for and conducting EW in support of assigned missions.

(g) Supporting other combatant commanders for the planning and integration of joint OPSEC and MILDEC.

3. Joint Information Operations Organizational Roles and Responsibilities

a. **Joint Staff.** The Chairman's responsibilities for IO are both general (such as those to establish doctrine, provide advice, and make recommendations) and specific (such as those assigned in DOD IO policy). The J-3 serves as the Chairman's focal point for IO and coordinates with the other organizations within the Joint Staff that have direct or supporting IO responsibilities. The IO divisions of the Joint Staff J-3 provide IO specific advice and advocate Joint Staff and combatant commands' IO interests and concerns within DOD and interact with other organizations and individuals on behalf of the Chairman. CJCSI 3210.01 Series, *Joint Information Operations Policy*, provides specific policy guidance on IO responsibilities and functions of the Joint Staff.

b. **Combatant Commands**

(1) CDRUSSTRATCOM's specific authority and responsibility to coordinate IO across AOR and functional boundaries does not diminish the imperative for the other combatant commanders to coordinate, integrate, plan, execute, and employ IO. These efforts may be directed at achieving national or military objectives incorporated in TSCPs, shaping the operational environment for potential employment during periods of heightened tensions, or in support of specific military operations. It is entirely possible that in a given theater, the combatant commander will be supported for select IO while concurrently supporting United States Strategic Command (USSTRATCOM) IO activities across multiple theater boundaries. As with other aspects of joint operations, joint IO should be accomplished through centralized planning and direction and decentralized execution. Joint-level planners should resist the temptation to plan in too great a level of detail. Plans that focus on objectives and end states rather than specific actions improve flexibility during execution and allow component staffs to develop plan details based on resource availability, constraints, and other factors. The specifics of planning IO as an integral part of joint plans are discussed in Chapter V, "Planning and Coordination."

(2) The Commander, US Special Operations Command (USSOCOM) shall, in addition to the responsibilities in section 2.b.(1) above, integrate and coordinate DOD PSYOP capabilities to enhance interoperability and support USSTRATCOM's IO responsibilities and other combatant commanders' PSYOP planning and execution. USSOCOM shall also employ other SOF IO capabilities as directed.

c. **Components.** Components are normally responsible for detailed planning and execution of IO. IO planned and conducted by the components must be conducted within the parameters established by the JFC. At the same time, component commanders and their subordinates must be provided sufficient flexibility and authority to respond to local variations in the information environment. Component

commanders determine how their staffs are organized for IO, and normally designate personnel to liaise between the JFC's headquarters and component headquarter staffs.

d. **Subordinate JFCs.** Subordinate JFCs plan and execute IO as an integrated part of joint operations. Subordinate staffs normally share the same type of relationship with the parent joint force IO staff as the Service and functional components. **Subordinate JFC staffs may become involved in IO planning and execution to a significant degree**, to include making recommendations for employment of specific capabilities, particularly if most of the capability needed for a certain operation resides in that subordinate JTF.

4. Organizing for Joint Information Operations

The principal staffs that may be involved in IO planning are the **combatant command**, **subordinate joint force command(s)**, and **component staffs**.

a. **Combatant Command Organization. Combatant command staffs,** supported by the IC and other DOD combat support agencies and Department of State (DOS) 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 JOPES to carry out planning responsibilities. The command which is designated the supported command receives guidance and support from the President and SecDef and can call on the expertise and technical support of all other designated supporting commands.

(1) Combatant commanders normally **assign responsibility for IO** to the **J-3**. When authorized, the director of the J-3 has primary staff responsibility for planning, coordinating, integrating, and assessing joint force IO.

(2) **IO Cell Chief. The J-3 normally designates an IO cell chief** to assist in executing joint IO responsibilities. The IO cell chief is the central point of contact on the combatant command staff for IO. The primary function of the IO cell chief is to ensure that IO are integrated and synchronized in all planning processes of the combatant command staff and that IO aspects of such processes are coordinated with higher, adjacent, subordinate, and multinational staffs. In operational planning, the IO cell chief ensures that the IO portions of JOPES and TSCP products reflect the combatant commander's guidance and are consistent with the operational principles and elements of operational design discussed in JP 3-0, *Joint Operations*, and Chapter V, "Planning and Coordination," in this publication. The IO cell chief is normally responsible for functions shown in Figure IV-1.

(3) **IO Staff.** The IO cell chief is normally assigned responsibility for supervision of IO activities for that portion of the J-3 staff designated as IO planners and for coordination with SMEs within the joint force. The portion of the staff under the cognizance of the IO cell chief is normally given a specific numerical designation such as "J-39." This staff section assists the IO cell chief and provides IO planning and core capability expertise within the staff and coordinates with other staffs and supporting agencies and organizations. During the **execution** of an operation, IO planners shall be available to the joint operations center (JOC) or its equivalent to assist in integration, deconfliction, support, or adjustment

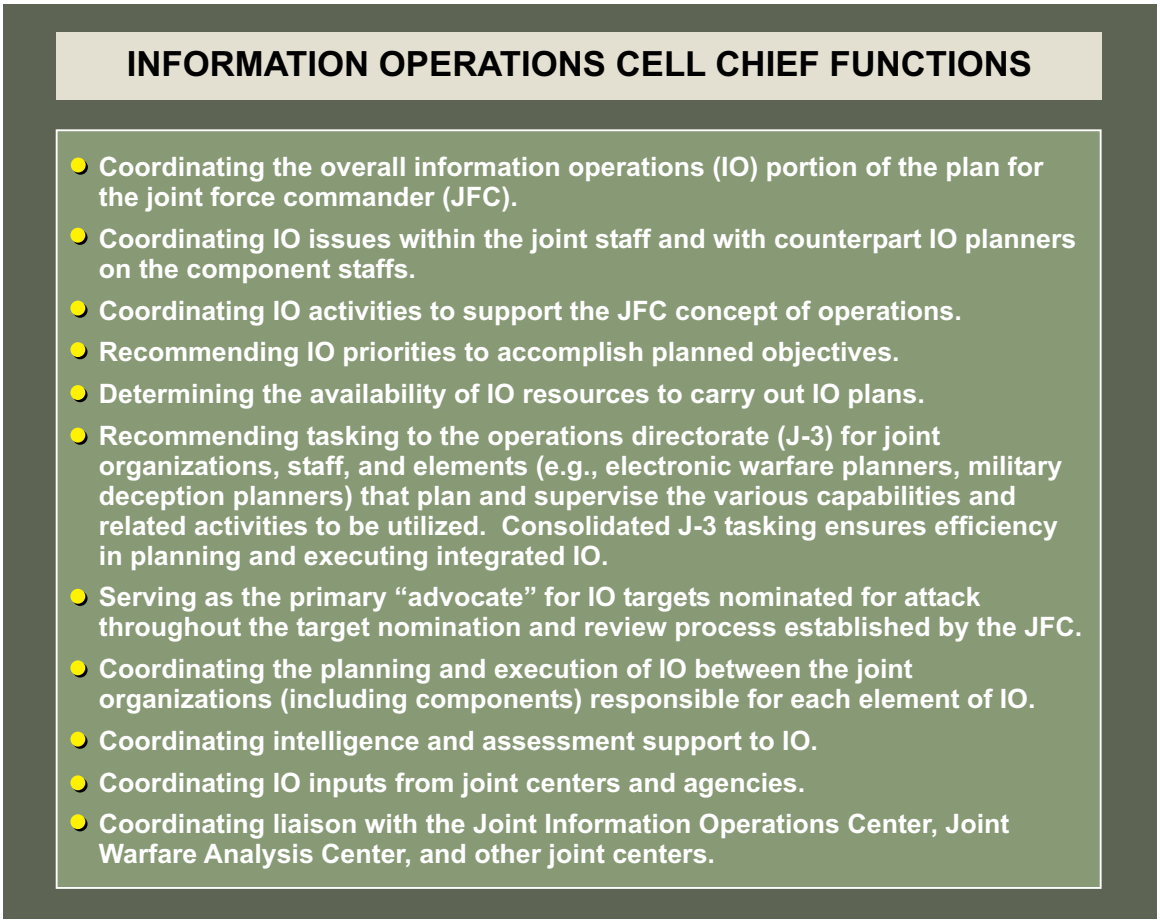


Figure IV-1. Information Operations Cell Chief Functions

of IO activities as necessary. If IO manning permits and the J-3 or IO cell chief designates, **IO staff personnel may be part of the JOC watch team** or stand a separate watch. Due to the sensitive nature of some aspects of IO, all members of the IO staff should have the appropriate security clearance and access necessary to fulfill their IO responsibilities.

(4) **IO Cell or Planning Organization.** To integrate and synchronize the core capabilities of IO with IO-supporting and related capabilities and appropriate staff functions, the IO cell chief normally leads an "IO cell" or similarly named group as an integrated part of the staff's operational planning group or equivalent. The organizational relationships between the joint IO cell and the organizations that support the IO cell are per JFC guidance. **These supporting organizations provide guidance** on the employment of their respective capabilities and activities. The specific duties and responsibilities of representatives from these supporting organizations should be established between the IO cell chief and the senior representative of each supporting organization. **Authorized staffing levels**, **mission**, and **location of JFC staff vis-à-vis each capability-level organization** are among the considerations in determining how organizations are represented in the cell. Figure IV-2 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. Capability, staff function and organizational representation on the IO cell may include the following personnel listed and described below.

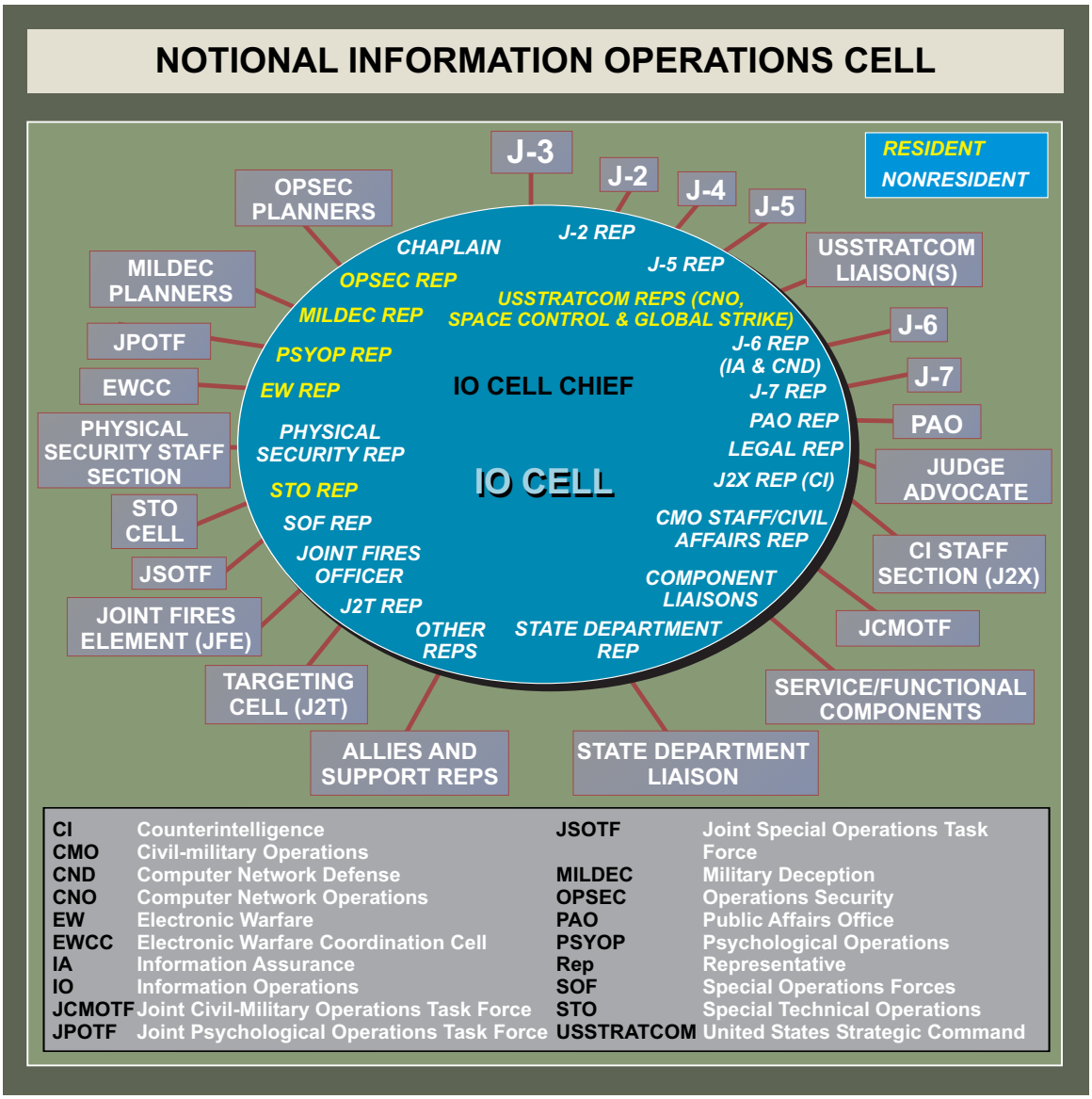


Figure IV-2. Notional Information Operations Cell

(a) **EW Representative.** Coordinates **EW activities and acts as liaison between the IO cell and the EWCC when formed (at the direction of the JFC)**. Serves as **Joint Spectrum Center (JSC) liaison officer** and provides oversight of input and changes to the JRFL in the absence of an EWCC. When directed by the JFC, the EWCC will stand up and reside at the JFC component most appropriate to the ongoing operation, and will be directly responsible to the JFC, through the EW representative in the IO cell, for the coordination and deconfliction of all EW activities and all military usage of the EM spectrum within the combatant commander's AOR. When an EWCC is active, the EWCC chief or his designated representative should be the EW representative at the IO cell. Coordinates closely with J-6 planners to deconflict friendly IO in the EM spectrum.

(b) **CNO Representative.** Coordinates integration and synchronization of CNO with other IO capabilities and deconflicts CNO with other staff directorates and organizations

represented in the IO cell.

(c) **PSYOP Representative.** Coordinates to provide DSPD. Integrates, coordinates, and synchronizes the use of **PSYOP** with other IO capabilities, functions, agencies, and organizations represented in the IO cell. Serves as entry point for liaison from the JPOTF, the in-theater multinational PSYOP cells, and Joint PSYOP support element as appropriate.

(d) **OPSEC Representative.** With assistance from each directorate, identifies existing threats and vulnerabilities, develops the critical information list, and implements OPSEC countermeasures. Serves as the joint communications security (COMSEC) monitoring activity (JCMA) point of entry into the staff.

(e) **MILDEC Representative.** Coordinates combatant command or subordinate joint force command MILDEC planning.

(f) **Special Technical Operations (STO) Representative.** The STO representative should be an integral member of the IO cell to ensure STO planning is fully integrated and coordinated. STO read-ins are conducted throughout the IO staff based on mission requirements and governing security directives.

(g) **USSTRATCOM Representative(s).** Participates via collaborative systems or in person when available. Acts as liaison to USSTRATCOM across AOR or functional boundaries to support IO planning and execution.

(h) **J-6 Communication Systems and IA Representative.** Facilitates **IA and coordination** between information system planners and managers and members of the IO cell. Coordinates with the J-3 to **minimize IO operations impact** on friendly forces C2. Principal liaison with the joint network operations control center (JNCC). Identifies critical information systems and vulnerabilities of these systems and networks (non-secure internet protocol router network, SECRET Internet Protocol Router Network [SIPRNET], Joint Worldwide Intelligence Communications System, voice, video, data, satellite, and tactical communications). May assist coordination between the J-3 and OPSEC planners with JCMA.

(i) **J-2 Representative.** Coordinates **collection requirements** and **analytical support** for compartmented and noncompartmented IO. May serve as liaison to the IO cell for other DOD intelligence agencies. Provides baseline assessment of the information environment.

(j) **Targeting Cell Representative.** Represents the **targeting cell(s)** and **coordinates IO targets** with the joint targeting coordination board (JTCB), if designated.

(k) **CI Representative.** Coordinates **IO inputs to CI activities** which have significant roles in IO. Provides input on adversary collection capabilities for OPSEC planning.

(l) **Physical Security Representative.** Provides physical security expertise and advocates interests and concerns within the joint command, the host base, and the joint rear area as

appropriate, during IO cell planning deliberations. May liaise between the IO cell and both the joint rear tactical operations center and the base defense operations center when appropriate.

(m) **Logistics Directorate (J-4) Representative.** Coordinates and integrates **IO logistic considerations** into the contingency planning process. Represents IO cell concerns to the time-phased force and deployment data (TPFDD) process and assists IO cell members in getting IO capabilities properly entered and synchronized on the time-phased force and deployment list (TPFDL). During deployment, execution, and redeployment phases of an operation, the J-4 representative can assist IO cell members in tracking movement of IO activities and their logistic support to and from the supported AOR. The J-4 representative relays IO planning guidance for OPSEC to other J-4 staff personnel and provides logistic policy guidance as appropriate.

(n) **Plans Directorate Representative.** Coordinates integration and synchronization of IO cell procedures and products into staff operational and theater planning processes.

(o) **Operational Plans and Joint Force Development Directorate (J-7) Representative.** Provides **exercise planning, modeling and simulation (M&S), and lessons learned process expertise and advocates exercise planning, M&S, and lessons learned interests and concerns**. 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 Lessons Learned Program**, as appropriate.

(p) **PA Representative.** Coordinates **and deconflicts PA activities with planned IO**.

(q) **CMO Representative.** Ensures **consistency of CMO activities** within the combatant commander's AOR that may support IO. Provides IO cell cultural advice and analysis of IO impact on civilian targets. Coordinates IO support to CMO as required. Provides interagency coordination, intergovernmental coordination, and coordination with nongovernmental organizations (NGOs), and host nations. Provides feedback on IO MOEs.

(r) **Judge Advocate (JA) Representative.** Advises planners to **ensure IO complies with domestic and international law** and assists with interagency coordination and negotiation.

(s) **Special Operations Representative.** Coordinates **use of SOF** within an AOR or joint operations area in support of IO.

(t) **Service and Functional Component Representatives.** These officers interface with the combatant command IO cell to provide component expertise and act as a liaison for IO matters between the combatant command 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). For most effective coordination between the combatant command IO cell and the component IO cells, the liaisons must be pre-designated, thoroughly familiar with the component's IO plan, and of the appropriate rank to speak for the component when the component is at a separate location.

(u) **Chaplain Representative.** Chaplains, as noncombatants, should not participate in combatant activities that might compromise their noncombatant status; however, they may provide relevant information on the religious, cultural, and ideological issues at the strategic and operational levels.

(v) **DOS Representative.** DOS will coordinate with foreign and international organizations that could be or are affected by the implementation of IO activities. Provides **PD expertise and advocates PD and DOS interests and concerns** during IO cell planning deliberations. The DOS representative provides a view of the PD capabilities that can be brought to bear to achieve USG objectives within the military operational area, and makes recommendations for interacting with civilian (and military) leaders, which can influence the outcome of military operations.

(w) **Support Organization Representatives.** Representatives from various organizations providing support to IO, discussed in paragraph 4.c. below and not mentioned specifically above, may participate in IO cell planning deliberations as directed in individual joint staff procedures and standing operating procedures (SOPs).

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

b. **Joint Task Force Command Organization**

(1) The size of the IO staff, at the JTF level, is determined by the JTF commander based on a variety of factors including assigned mission and available resources. The standing joint force headquarters core element (SJFHQ CE) is a part of each geographic combatant commander's staff that provides a trained and equipped standing, joint C2 element specifically organized to conduct joint operations. It facilitates JTF headquarters (HQ) formation either as an integrated part of the JTF commander's HQ or from its location at the combatant commander's HQ. If elements of the SJFHQ CE deploy, they become an integral part of the JTF HQ, not a separate organization within the JTF HQ. SJFHQ CEs have IO sections that benefit from the SJFHQ CE's cross-functional organization and planning methodology.

(2) The primary purpose of a JTF IO staff is to focus IO planning and support within the JTF HQ. The JTF IO staff provides expertise to the other JTF HQ staff directorates and is the focal point for coordinating and deconflicting individual core, supporting and related IO capabilities with other staff functions, component and higher HQ staff, and supporting agencies and organizations. JTF IO staff's responsibilities include:

(a) Participation in JTF planning.

(b) Integration and synchronization of IO core, supporting, and related capabilities within the JTF. Processes are discussed in paragraph 5 below and in Chapter V, "Planning and Coordination."

(c) Oversight of the IO aspects of the JTF commander's assigned missions.

c. **Organization of Support for IO.** As discussed above, **IO planners use other joint organizations to plan and integrate joint IO**. Support for IO comes primarily from within DOD, but other government agencies and organizations, as well as some allied agencies and organizations, may support IO.

(1) Support from within DOD includes, but is not limited to, personnel augmentation from the **Service IO organizations, USSTRATCOM's Joint Information Operations Center, USSOCOM, US Joint Forces Command (USJFCOM) Joint Warfare Analysis Center (JWAC), Joint Program Office for Special Technology Countermeasures (JPO-STC)**, **JSC**, and **JCMA**. Additionally, through the various joint organizations that plan and direct core, supporting, and related IO capabilities, **commanders and planners have access to the component expertise** necessary to plan the employment or protection of component systems or units.

(a) **National Geospatial-Intelligence Agency (NGA).** NGA support for IO may be coordinated through the J-2 representative of the IO cell or directly with a NGA representative and can include:

1. Determination of the availability of the various types of existing geospatial reference data covering the area of interest.

2. Deconfliction of national and lower-level geospatial intelligence (GEOINT) collection activities.

3. GEOINT data and products describing the physical environment and the adversary's locations, capabilities, limitations, and vulnerabilities.

4. Geospatial data quality information (accuracy, currency, completeness, consistency) and appropriateness of the data for the intended use.

5. Visualization and spatial/spectral analysis of imagery and geospatial information in support of mission planning, rehearsal, execution, and post-mission assessment.

6. Disclosure and release of GEOINT to allies and coalition partners.

(b) **National Security Agency (NSA).** NSA support for IO may be coordinated through the J-2 representative of the IO cell or directly with a NSA representative and can include:

1. Information security technology, products, and services.

2. Vulnerability and threat analyses to support IA and the defense of US and friendly information systems.

3. Determining exploitation risk for telecommunications systems.

4. Determining releasability of COMSEC materials to allies or coalition partners.

5. Providing technical expertise for CNO.

6. Conducting intelligence gain/loss assessments.

7. Collecting C2 targeting-related information.

(c) **Defense Intelligence Agency (DIA).** DIA support for IO may be coordinated through the J-2 representative of the IO cell or directly with the DIA representative to include:

1. Intelligence for IO target selection and post-strike analysis.

2. Identifying friendly vulnerabilities and the most probable friendly targets within the adversary's capabilities and concept of operations.

3. Developing all-source intelligence gain/loss and/or risk assessment of IO targets.

4. Conducting political, military, and human factors assessments.

(d) **Defense Information Systems Agency (DISA).** DISA support for IO may be coordinated through the J-6 representative of the IO cell or directly with the DISA representative and includes:

1. Coordinating with DIA, NSA, and the Services to ensure sufficient database support for planning, analysis, and execution of IO.

2. Assisting in disseminating adversarial CNA warnings.

3. Assisting in establishing a security architecture and standards for protecting and defending selected portions of the Global Information Grid.

4. Developing IA education, training, and awareness program guidelines, including minimum training standards, for use by the JTF HQ, components, and subordinate JTFs.

(e) **JWAC.** The JWAC assists the combatant commanders in their preparation and analysis of joint operation plans (OPLANs) 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 supports a JTF through the supported combatant commander. See Appendix A, "Supplemental Guidance," (published separately).

(f) **JPO-STC.** The JPO-STC provides the combatant commanders, Service Chiefs, and operating forces with the **ability to assess their critical infrastructure protection dependencies and the potential impact on military operations** resulting from disruptions to key infrastructure components (e.g., electric power, natural gas, liquid petroleum, transportation, and telecommunications). JPO-STC also conducts **technical assessments of emerging special technologies** to determine their potential impacts on military and civilian systems and proposes countermeasure solutions and/or response options. See Appendix A, "Supplemental Guidance," (published separately).

(g) **JSC.** The JSC can provide the following direct support to the JFC through the EWCC or the EW representative to the IO cell.

1. Locational and technical characteristics about friendly force C2 systems.

2. Augmentation teams trained to prepare a JRFL or provide training and assistance in how to prepare a JRFL.

3. Augmentation teams trained to prepare a JRFL to locate and identify interference sources and recommend technical and operational fixes to resolve identified interference sources or to provide training and assistance.

4. Assistance in the resolution of operational interference and jamming incidents.

5. Data about foreign communications systems frequency and location.

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

(h) **JCMA.** The JCMA can provide the following direct support to the JFC through the IO cell:

1. COMSEC monitoring and analysis support.

2. A joint COMSEC monitoring and analysis team to provide direct, deployable joint COMSEC monitoring support. If tasked, the JCMA may manage all COMSEC monitoring.

3. Cryptographic or plain language system monitoring.

4. Timely, tailored reporting to supported commanders, to include near real time reporting of inadvertent disclosure of friendly critical information identified in the OPSEC process.

(i) **Joint Communications Support Element (JCSE).** JCSE is a rapidly deployable, joint tactical communications unit under the OPCON of USJFCOM that provides contingency and crisis communications to joint forces. JCSE is composed of Active and Reserve Component forces and is equipped with a wide array of tactical and commercial communications equipment. JCSE supports time-sensitive operations.

(2) **Interagency Support.** Non-DOD USG departments and agencies may have a role in planning and executing IO. The expertise, programs, and activities of a wide variety of non-DOD USG agencies should be **considered as part of the IO plan when appropriate**. Combatant commanders establish staff procedures specific to their AOR for requesting interagency support and coordination of various aspects of joint operations. For more discussion on interagency coordination, see JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations, Volume I*. Normally combatant commanders work through designated liaison representatives attached to their command. USSTRATCOM can assist joint commanders in requesting interagency IO support when liaison representatives from specific organizations are not attached. Planning coordination of IO as an integral part of planning joint operations is discussed in Chapter V, "Planning and Coordination." The following departments, agencies, and organizations are not all inclusive but representative of possible interagency support and coordination required for IO.

(a) **DOS.** DOS will coordinate with foreign and intergovernmental organizations that could be or are affected by the implementation of an IO plan. See Volume II of JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations*.

(b) **Other Representatives and Liaison Officers.** The JFC should tailor the composition of the cell as necessary to accomplish the mission. Other representatives could include, for example, the non-DOD intelligence community. See Volume II of JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations*.

(3) **Multinational Support.** Chapter VI, "Multinational Considerations in Information Operations," discusses multinational support of IO. See also AJP-3 for North Atlantic Treaty Organization specific doctrine.

CHAPTER V
PLANNING AND COORDINATION

"Master the mechanics and techniques; understand the art and profession; and be smart enough to know when to deviate from it."

Gen Anthony Zinni, CDRUSCENTCOM
1997-2000

1. Introduction

IO planning follows the principles and processes established for joint operation planning. The IO staff coordinates and synchronizes capabilities to accomplish JFC objectives. Uncoordinated IO can compromise, complicate, negate, or harm other JFC military operations, as well as other USG information activities. JFCs must ensure IO planners are fully integrated into the planning and targeting process, assigning them to the JTCB in order to ensure full integration with all other planning and execution efforts. Other USG and/or coalition/allied information activities, when uncoordinated, may complicate, defeat, or render DOD IO ineffective. Successful execution of an information strategy also requires early detailed JFC IO staff planning, coordination, and deconfliction with USG interagency efforts in the AOR to effectively synergize and integrate IO capabilities.

2. Information Operations Planning

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

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

c. IO planning requires early and detailed preparation. Many IO capabilities require long lead-time intelligence preparation of the battlespace (IPB). IO support for IPB development differs from traditional requirements in that it may require greater lead time and may have expanded collection, production, and dissemination requirements. Consequently, combatant commanders must ensure that IO objectives are appropriately prioritized in their priority intelligence requirements (PIRs) and requests for information (RFIs). In addition, the intelligence gain/loss from the application of an IO capability and the status of the target as a viable element of the target system must be evaluated by the IC prior to execution.

d. As part of the planning process, designation of release and execution authority is required. Release authority provides the approval for IO employment and normally specifies the allocation

of specific offensive means and capabilities provided to the execution authority. Execution authority is described as the authority to employ IO capabilities at a designated time and/or place. Normally, the JFC is the one execution authority designated in the execute order for an operation.

See Appendix A, "Supplemental Guidance," (published separately), for additional guidance.

e. **Legal Considerations in IO. IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval.** The United States constitution, US laws, and international law set boundaries and establish precedence for military activity in the information environment. Another country's legal basis and limitations for military activity in the information environment may differ. US military activities in the information environment, as in the physical domains, are conducted as a matter of law and policy. US forces, whether operating physically from bases or locations overseas or virtually in the information environment from within the boundaries of the US or elsewhere, are required by law and policy to act in accordance with US law and the LOAC.

(1) Legal limitations may be placed on IO. All military activities in the information environment are subject to the LOAC. In order to determine whether there are any questions of the legality of particular IO tasks, such tasks must be reviewed by the appropriate JA and approved by appropriate levels of the chain of command. Bilateral agreements to which the US is a signatory may have provisions concerning the conduct of IO and its supporting, or related capabilities and should be consulted prior to action. A current list of treaties and other international agreements in force is found in Department of State Publication 9434, *Treaties In Force*.

(2) IO planning at all levels should consider the following broad areas and consult the appropriate personnel for input:

(a) Whether a particular use of IO may be considered a hostile act by other countries.

(b) Domestic, international, criminal, and civil law, affecting national security, privacy, and information exchange.

(c) International treaties, agreements, and customary international law, as applied to IO.

(d) Structure and relationships among US intelligence organizations and the overall interagency environment, including NGOs.

3. Information Operations Planning Considerations

This section is an overview of IO as a part of the joint operation planning processes and products, with a focus on common planning activities**.** The joint planning process steps are: planning initiation; mission analysis; COA development; COA analysis and wargaming; COA comparison; COA approval; and plan or order development. A more detailed discussion of the planning process can be found in JP

5-0, *Joint Operation Planning*. Figure V-1 shows the IO cell actions and outcomes aligned with the joint operation planning process and steps.

a. **Planning Initiation.** Integration of IO into joint operations should begin at the initiation of planning. Key IO staff actions during this phase are:

(1) Monitor the situation and receive initial planning guidance, review staff estimates from applicable OPLANs and/or operation plans in concept format.

(2) Convene the IO cell. The cell should use this opportunity to alert subordinate commands/units of potential tasking with regard to IO planning support. For crisis action planning, regularly convene to review the situation and determine what preliminary planning actions should be accomplished. For contingency planning, convene a meeting of the full IO cell or consult informally with other members as needed.

(3) Gauge initial scope of the IO role in the operation.

(4) Identify location, SOP, and routine of other staff organizations that require IO interaction and divide coordination responsibilities among IO staff.

(5) Begin identifying information needed for mission analysis and COA development and availability of required information. (Continues through plan development.)

(6) Identify IO planning support requirements (including staff augmentation and support products and services) and issue requests for support according to procedures established locally and by various supporting organizations.

(7) Validate, initiate, and revise PIRs and RFIs, keeping in mind the long lead times associated with satisfying IO requirements. (Continues throughout contingency planning process.)

(8) Provide input and recommendations on IO strategies and resolutions to conflicts with other plans.

(9) Submit IO target nominations to JFC or component JTCB for IC review of intelligence gain/loss, and for JFC deconfliction and validation.

(10) Ensure IO planners participate in all JFC or component planning and targeting sessions, JTCBs, and/or Joint Effects Coordination Boards.

b. **Mission Analysis.** The purpose of mission analysis is to assess the assigned mission in order to determine the commander's objectives and tasks, and to prepare guidance for subordinate elements. Key IO staff actions during this phase are:

(1) Identify specified, implied, and essential IO tasks.

INFORMATION OPERATIONS CELL ACTIONS AND OUTCOMES AS PART OF JOINT PLANNING

PLANNING PROCESS STEPS	IO CELL PLANNING ACTION	IO CELL PLANNING OUTCOME
Planning Initiation	Monitor situation. Review guidance and estimates. Convene IO cell. Gauge initial scope of the IO role. Identify organizational coordination requirements. Initiate identification of information required for mission analysis and COA development. Validate, initiate, and revise PIRs/RFIs. Recommend IO strategies and conflict resolution.	Request taskings to collect required information.
Mission Analysis	Identify specified, implied, and essential IO tasks. Identify assumptions, constraints, and restraints relevant to IO. Identify IO planning support requirements (including augmentation) and issue requests for support. Initiate development of MOEs and MOPs. Analyze IO capabilities available and identify authority for deployment and employment. Identify relevant physical, informational and cognitive properties of the information environment. Refine proposed PIRs/RFIs. Provide IO perspective in the development of restated mission for commander's approval. Tailor augmentation requests to missions and tasks.	List of IO tasks. List of assumptions, constraints, and restraints. Planning guidance for IO. IO augmentation request. IO portion of the commander's restated mission statement.
COA Development	Select IO core, supporting, and related capabilities to accomplish IO tasks for each COA. Revise IO portion of COA to develop staff estimate. Provide results of risk analysis for each COA.	List of objectives to effects to IO tasks to IO capabilities for each COA.
COA Analysis & Wargaming	Analyze each COA from an IO functional perspective. Identify key IO decision points. Recommend IO task organization adjustments. Provide IO data for synchronization matrix. Identify IO portions of branches and sequels. Identify possible high-value targets related to IO. Recommend IO CCIRs.	IO data for overall synchronization matrix. IO portion of branches and sequels. List of high-value targets related to IO.
COA Comparison	Compare each COA based on mission and IO tasks. Compare each COA in relation to IO requirements versus available IO resources. Prioritize COAs from an IO perspective.	Prioiritized COAs from an IO perspective with Pros and Cons for each COA.
COA Approval	No significant IO staff actions during COA approval.	N/A

Figure V-1. Information Operations Cell Actions and Outcomes as Part of Joint Planning

INFORMATION OPERATIONS CELL ACTIONS AND OUTCOMES AS PART OF JOINT PLANNING (cont'd)

PLANNING PROCESS STEPS	IO CELL PLANNING ACTION	IO CELL PLANNING OUTCOME
Plan or Order Development	Refine IO tasks from the approved COA. Identify IO capability shortfalls and recommend solutions. Update continually, all supporting organizations regarding details of the IO portion of plan details (access permitting). Advise supported combatant commander on IO issues and concerns during supporting plan review and approval. Participate in TPFDD refinement to ensure the IO force flow supports the CONOPS.	Updated IO estimates based on selected COA. Draft IO appendices and tabs, supporting plans. IO requirements to TPFDD development. Synchronized and integrated IO portion of operation plan.
Plan Refinement	No specific IO staff actions during plan refinement.	N/A

CCIR	Commander's Critical Information Requirement	MOE	Measure of Effectiveness
COA	Course of Action	MOP	Measure of Performance
CONOPS	Concept of Operations	PIR	Priority Intelligence Requirement
IO	Information Operations	RFI	Request for Information
		TPFDD	Time Phased Force Deployment Data

Figure V-1. Information Operations Cell Actions and Outcomes as Part of Joint Planning (cont'd)

(2) Identify assumptions, constraints, and restraints relevant to IO.

(3) Initiate development of MOEs and measures of performance (MOPs).

(4) Analyze IO capabilities available for the mission and identify level of approval authority for deployment and employment.

(5) Identify relevant physical, informational, and cognitive properties (whether friendly, adversarial or neutral/third party) of the information environment that may impact the operation. Commanders and their staffs must avoid projecting US value sets on opponents (mirror imaging). Therefore, incorporating specific cultural, regional, and country experts into the IO planning process can help prevent developing plans based on inaccurate cultural assumptions.

(6) Refine proposed PIRs and RFIs.

(7) Provide IO perspective in development of restated mission for the commander's approval.

(8) Tailor the quantity and skill sets in augmentation requests to the specifics of mission and tasks as they are developed.

(9) Based on intelligence and mission analysis, identify potential IO targets, compile an IO target development list, and nominate developed IO targets to the JFC's standing joint target list.

(10) Compile and maintain a target folder for each IO target nomination incorporating at least the minimum data fields set by the Military Targeting Committee. Target folders will facilitate IC review and JFC deconfliction and commander approval for action.

c. **COA Development.** The staff takes the output from mission analysis as key inputs to COA development: initial staff estimates; mission and tasks; and JFC planning guidance. Key IO staff actions during this phase are:

(1) Select IO core capabilities that may be used individually or integrated with other options to accomplish IO supporting tasks for each COA.

(2) Revise the IO portion of COAs as required to develop the staff estimate.

(3) Brief portions of each COA and include the results of risk analysis for each COA.

d. **COA Analysis and Wargaming.** Based upon time available, the commander should wargame each tentative COA against adversary COAs identified through the JIPB process. Key IO staff actions during this phase are:

(1) Analyze each COA from an IO functional perspective.

(2) Reveal key IO decision points.

(3) Recommend IO task organization adjustments.

(4) Provide IO data for use in a synchronization matrix or other decision-making tool.

(5) Identify IO portions of branches and sequels.

(6) Identify possible high-value targets related to IO.

(7) Recommend commander's critical information requirement for IO.

e. **COA Comparison.** COA comparison starts with all staff members analyzing and evaluating the advantages and disadvantages of each COA from their perspectives. Key IO staff actions during this phase are:

(1) Compare each COA based on mission and IO tasks.

(2) Compare each COA in relation to IO requirements versus available IO resources.

(3) Prioritize COAs from an IO perspective.

f. **COA Approval.** There are no significant IO staff actions during COA approval.

g. **Plan or Order Development.** During plan or order development, the IO staff develops the IO portion of the plan or order. Key IO staff actions during this phase are:

(1) Refine IO tasks from the approved COA.

(2) Identify IO capability shortfalls and recommend solutions.

(3) Facilitate development of supporting plans by keeping organizations responsible for development of supporting plans informed of IO plan development details (as access restrictions allow) throughout the planning process.

(4) Advise the supported combatant commander on IO issues and concerns during the supporting plan review and approval process.

(5) Participate in TPFDD refinement to ensure the IO force flow supports the OPLAN.

h. **Plan Refinement.** There are no IO specific staff actions during plan refinement.

4. Commander's Intent and Information Operations

The commander's vision of IO's role in an operation should begin before the specific planning is initiated. A commander that expects to rely on IO capabilities must ensure that IO related PIRs and RFIs are given high enough priority prior to a crisis, in order for the intelligence products to be ready in time to support operations. At a minimum, the commander's vision for IO should be included in the initial guidance. Ideally, commanders give guidance on IO as part of their overall concept, but may elect to provide it separately. The commander may elect to provide separate guidance on IO when a more focused and direct discussion about IO is appropriate. Commanders may find providing separate guidance on IO during exercises is a valuable tool for training their staffs to view IO as an integral part of their overall operations concept.

5. The Relationship Between Measures of Performance and Measures of Effectiveness

a. **MOPs** gauge accomplishment of IO tasks and actions. **MOEs** determine whether IO actions being executed are having the desired effect toward **mission accomplishment**: the attainment of end states and objectives. MOPs measure friendly IO effort and MOEs measure battlespace results. The relationship between these two measures is illustrated by examples in Figure V-2. IO MOPs and MOEs are crafted and refined throughout the planning process.

b. In developing IO MOPs and/or MOEs, the following general criteria should be considered:

(1) **Ends Related.** They should directly relate to desired effects required to accomplish objectives.

(2) **Measurable.** Effectiveness or performance is measured either quantitatively or qualitatively. In order to measure effectiveness, a **baseline** measurement must be established prior to the execution, against which to measure system changes.

(3) **Timely.** The required feedback time should be clearly stated for each MOE and/or MOP and a plan made to report within specified time periods.

(4) **Properly Resourced.** The collection, collation, analysis, and reporting of MOE or MOP data requires personnel, budgetary, and materiel resources. IO staffs should ensure that these resource requirements are built into the IO plan during its development.

EXAMPLE OF THE RELATIONSHIP BETWEEN MEASURES OF PERFORMANCE AND MEASURES OF EFFECTIVENESS

Capability	Measures of Performance (MOPs)*	Measures of Effectiveness (MOEs)**	Remarks
Psychological Operations (PSYOP)	Percentage of PSYOP products disseminated	Extent that PSYOP changed the demonstrated behavior of the target audience	Often necessitates further intelligence requirements
Electronic Warfare (EW)	Percentage of adversary command and control (C2) facilities attacked	Effect of attacks on adversary C2 facilities' ability to pass critical information	MOE requires a change in a detectable and measurable activity
Operations Security (OPSEC)	Percentage of identified compromises of critical information or indicators with OPSEC measures applied	Observed adversary actions indicating lack of foreknowledge of friendly operations	MOE requires collation of all leaked information and comparison with adversary actions
Military Deception (MILDEC)	Days between updates on effectiveness of deception plans	Specific adversary actions taken based on friendly deception activities	MOE requires an estimate of how the adversary is expected to react if they do and if they do not believe the deception
Computer Network Operations (CNO)	Percentage of tasked network attacks conducted	Effect of network attacks on target systems	MOE requires access to a measurable output or to the adversary's own reporting of the attack

*MOPs are derived from CJCSM 3500.04D, Universal Joint Task List (UJTL). Most MOP are answered by internal statistic generation.

**MOEs vary and are based on IO objectives and individual planned tasks.

Figure V-2. Example of the Relationship Between Measures of Performance and Measures of Effectiveness

c. Examples of IO MOPs:

(1) Number of PSYOP products disseminated (weekly, monthly).

(2) Percentage of adversary command and control facilities attacked.

(3) Percentage of tasked CNAs conducted.

(4) Number of CMO projects initiated.

(5) Increased adversary radio transmissions within a desired frequency, due to EA.

(6) Human intelligence reports of PSYOP broadcasts during Commando Solo missions.

d. Examples of IO MOEs:

(1) Quantitative MOEs

(a) Percentage of degradation of a radar system over time as measured by an appropriate sensor.

(b) Number and size of civil disturbances over time as reported by own forces.

(c) Number of computer intrusions over time as measured by software.

(d) Trends in target population position on a specific issue as gauged by public opinion polls.

(e) Number of troops surrendering as instructed by a PSYOP leaflet operation.

(2) Qualitative MOEs

(a) Target population position on a specific issue as gauged by a focus group or series of focus groups.

(b) Assessment of changes in supportiveness (or non-supportiveness) of public statements made by key leaders as measured against IO objectives and/or effects.

(c) Assessment of changes in bias of foreign media outlets.

(d) Instances of defections, surrenders, non-support of authorities attributed to impact and/or credibility of loudspeaker broadcasts or leaflets.

e. **Challenges and Considerations.** It can be difficult to isolate variables and establish a direct cause and effect relationship, especially when assessing foreign public opinion or human behavior. Unforeseen factors lead to erroneous interpretations. For example, a traffic accident in a foreign country involving a US Service member and a local civilian may bias an audience against US policies irrespective of otherwise successful IO. Lack of leadership, equipment, weapons, or sustenance may have as great an influence on surrendering enemy soldiers as a PSYOP leaflet urging surrender. In contrast, a visit by a popular US official to a region may cause a positive spike in public opinion that cannot be credited to executed IO actions.

CHAPTER VI
MULTINATIONAL CONSIDERATIONS IN INFORMATION OPERATIONS

"We are a strong nation. But we cannot live to ourselves and remain strong."

George C. Marshall
22 January 1948

1. Introduction

Joint doctrine for multinational operations, including command and operations in a multinational environment, is described in JP 3-16, *Joint Doctrine for Multinational Operations*. The purpose of this chapter is to highlight IO-specific issues that are not covered in JP 3-16, Chapter IV, Section F "Information Operations." IO in a multinational environment are also covered in the US sponsored *America, Britain, Canada, and Australia Interoperability Program Coalition Operations Handbook*, Chapter 10. This document includes IO checklists for staff and commanders assigned to a multinational IO operational environment.

2. Other Nations and Information Operations

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

(1) Clarification of allied and coalition partners' IO objectives.

(2) Understanding of other nations' IO and how they intend to conduct these activities.

(3) Establishment of liaison/deconfliction procedures to ensure coherence.

(4) Early identification of MNF vulnerabilities and possible countermeasures to adversary attempts to exploit them.

b. Regardless of the maturity of each nation's IO capabilities, doctrine, tactics, techniques, or procedures, **every ally and/or coalition member can contribute to IO by** providing regional expertise to assist in planning and conducting IO. If allies and coalition partners have developed specific IO capabilities, such capabilities may be tailored to specific targets and threats in ways that are not utilized by the US. **Such contributions complement US IO expertise and capabilities,** and potentially enhance the quality of both the planning and execution of multinational operations.

3. Multinational Information Operations Considerations

a. Considerations in military operational planning processes, particularly for IO, whether JOPES-based or based on established foreign or alliance planning processes, should include:

(1) Recognizing allied/coalition partner cultural values and institutions.

(2) Recognizing allied/coalition partner interests and concerns.

(3) Recognizing differences between the US and foreign moral or ethical values.

(4) Understanding allied/coalition partners' rules of engagement and legal constraints concerning military activities in the information environment.

(5) Awareness of the complications of planning and execution in multiple languages and their effect on the time taken to develop and execute plans.

(6) Familiarity with allied/coalition partner IO doctrine, tactics, techniques, and procedures.

b. Sharing of information with allies and coalition partners.

(1) Each nation has various resources to provide both classified and unclassified information to a particular IO activity. In order to plan properly, all nations must be willing to share appropriate information to accomplish the assigned mission, but each nation is obliged to protect information that it cannot share with other nations.

(2) Information sharing arrangements in formal alliances, to include US participation in United Nations missions, are worked out as part of alliance protocols. Information sharing arrangements in ad hoc multinational operations where coalitions are working together on a short-notice mission, must be created during the establishment of the coalition.

(3) Using National Disclosure Policy (NDP) 1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*, and DODI O-3600.2, *Information Operations (IO) Security Classification Guidance (U)*, as guidance, the senior US commander in a multinational operation must provide guidelines to the US-designated disclosure representative on information sharing and the release of classified information or capabilities to allied/coalition forces. NDP 1 provides policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance. The disclosure of classified information is never automatic. It is not necessary for allied/coalition forces to be made aware of all US intelligence, capabilities, or procedures that are required for planning and execution of IO. The JFC should request approval from higher command authorities to release IO-related information that has not been previously cleared for allied/coalition partners.

(4) Information concerning US persons may only be collected, retained, or disseminated in accordance with law and regulation. Applicable provisions include: the Privacy Act, Title 5 US Code Section 552a; DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*; Executive Order 12333, *United States Intelligence Activities*; and DODD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*.

4. Planning, Integration, and Command and Control of Information Operations in Multinational Operations

a. The role of IO in multinational operations is the prerogative of the MNFC. The mission of the MNF determines the role of IO in each specific operation.

b. Representation of key allies/coalition partners in the MNF IO staff ensures multinational IO expertise and capabilities are effectively used, and the IO portion of the plan is coordinated with all other aspects of the multinational plan.

c. MNF members may not have IO capabilities, and it may be necessary for the MNF HQ to assist the subordinate MNFCs and their staffs in planning and conducting IO.

5. Multinational Organization for Information Operations Planning

a. When the JFC is also the MNFC, the joint force staff should be augmented by planners and SMEs from allied/coalition forces. Allied IO capability specialists should be trained on US and allied/coalition IO doctrine, requirements, resources, and how allied/coalition forces are structured to conduct IO. IO planners should seek to accommodate the requirements of each allied/multinational force, within given constraints, with the goal of using all the available IO expertise and capabilities of the multinational force.

b. In the case where the JFC is not the MNFC, it may be necessary for **the JFC J-3 to brief the MNFC and staff on the advantages of using US IO capabilities and procedures to achieve MNF goals**. The JFC should propose organizing a multinational IO staff using organizational criteria discussed earlier. If this is not acceptable to the MNFC, the JFC should assume responsibility for implementing IO within the joint force as a part of the multinational operations to support multinational mission objectives.

6. Multinational Policy Coordination

The development of capabilities, tactics, techniques, procedures, plans, intelligence, and communications support applicable to IO requires coordination with the responsible DOD components and allied/coalition nations. Coordination with allies above the JFC/MNFC level is normally effected within existing defense arrangements, including bilateral arrangements. **The Joint Staff coordinates**

US positions on IO matters delegated to them as a matter of law or policy, and discusses them bilaterally, or in multinational organizations, to achieve interoperability and compatibility in fulfilling common requirements. Direct discussions regarding multinational IO operations in specific theaters are the responsibility of the geographic combatant commander.

CHAPTER VII
INFORMATION OPERATIONS IN JOINT EDUCATION, TRAINING, EXERCISES, AND EXPERIMENTS

"The Romans are sure of victory . . . for their exercises are battles without bloodshed, and their battles bloody exercises."

Flavius Josephus
Historian, 37-100 AD

1. Introduction

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

2. Information Operations Education

As DOD conceptualization of the information environment and the role of IO in military affairs has evolved, the necessity of an IO career force has been realized. The basic tenets of education and training necessary for this force are:

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

b. **Initial capability specialist training and education requirements are Service and capability specific.** Capability specialists may be officers or enlisted. As Service-trained specialists become more experienced and senior, their training and education must be broadened to prepare them for responsibilities to plan and supervise the employment of other capabilities that are employed in IO, and to synchronize IO with other aspects of joint operations and USG policy.

c. **IO planners are required at both the component and the joint level.** Personnel assigned to IO planning must have a working knowledge of the various capabilities potentially

employed in IO as well as appropriate planning processes, procedures, tools, and the legal and policy basis for the conduct of IO.

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

3. Information Operations Training

a. Joint military training is based on joint policies and doctrine to prepare joint forces and/or joint staffs to respond to strategic and operational requirements deemed necessary by combatant commanders to execute their assigned missions. **The basic joint IO training task is to educate those personnel and organizations responsible for planning and conducting joint IO in the doctrine found in this and other joint publications.**

b. **IO training must support the IO career force and be consistent with the joint assignment process.** Joint IO training focuses on joint planning-specific skills, methodologies and tools, and assumes a solid foundation of Service-level IO training.

c. **The Services determine applicable career training requirements for both their IO career personnel and general military populations, based on identified joint force mission requirements**. Joint training requirements related to IO include both those recommended by the nature of the information environment and those specific to the planning and execution of IO.

(1) **Service-wide training of military personnel should account for the nature of the information environment** and the fact that the **actions of individual personnel can affect the perceptions of foreign populations**. The Services are responsible for sensitizing the entire military population to the potential impact of their individual and collective actions on the perceptions of foreign populations, particularly when visiting or assigned to overseas locations, where cultural values and institutions differ substantially from the US norm. **Prior to deployment to locations outside the US, military personnel should receive cultural-specific indoctrination. The objective of such indoctrination should be to prevent inadvertent misperceptions of US forces' actions and conduct by foreign populations at the deployed location.** Personnel expected to operate at length or covertly among foreign populations must receive more extensive cultural training.

(2) **Language and cultural skills are critical to IO.** Language training in the past has focused on intelligence requirements. Additionally, the requirement for cultural training is increasing. IO requires not only that appropriate messages and themes be translated accurately, but that joint forces have the language and cultural skills to understand how their actions and messages, intended and unintended, are being perceived by the populations among which they operate. **Misperception and misunderstanding are complicated and reinforced when joint forces do not have sufficient language and cultural skills to communicate effectively among the populations where they operate.** The burden of acquiring proficiency in a foreign language and culture cannot be placed primarily on the foreign population's ability to learn English and

Western culture. **Lack of sufficient language expertise and cultural understanding makes the joint force dependent on foreign translators.** Language training must provide sufficient numbers of personnel fluent in those languages and conversant in those cultures where joint forces expect to operate. Language and cultural skills are required for those forces to interact effectively with foreign populations and maintain awareness of foreign population perceptions during the course of any joint operation.

(3) **Specific IO capabilities, such as CND and OPSEC, also have training requirements that are applicable to the general military population on a continuing basis.** Such capabilities require an "all hands" effort and are dependent on individuals knowing the consequences of their mistakes or inactions in following "proper procedures."

(4) Beyond these basic military-wide training requirements, the training of IO capability specialists is a Service responsibility. **The development of specific capability expertise should be complemented by increasingly in-depth instruction appropriate to the student's seniority level. More in-depth training should broaden the student's perspective** of the role of specific IO capabilities and their impact on the conduct of joint operations. Such training requires reinforcement and enhancement throughout their careers. Only this continuity of Service training can provide the foundation necessary to build joint IO planners and indoctrinate future senior military leaders in the complexities and subtleties of military activity in the information environment.

(5) IO practitioners need education to help them learn how to think about IO. IO requires very detailed analysis and skilled synthesis, fueled by specific subject matter expertise and knowledge. IO requires its practitioners to synthesize and view problems/challenges as holistic and related instead of isolated. Hence, each part of IO relates to other parts, with actions in one part of the world affecting other geographical areas and dimensions. IO education must give people a broad appreciation of how different cultures affect how people think, plan, and interpret outcomes. IO planners also need education sufficient for conducting sophisticated wargaming going back and forth from the mind of the friendly commander to the minds of other participants in the conflict who have influence on friendly COAs.

4. Planning Information Operations in Joint Exercises

Effective employment of IO in joint operations depends on the ability of US forces to train as they intend to fight. Joint exercises provide a unique opportunity to rehearse and evaluate component IO capabilities in mutually supportive operations. **The complexity of integrating IO into joint operations, and the impact that IO potentially has on other aspects of joint operations, recommend the inclusion of IO in most joint exercises.**

a. Exercise planning is a separate process from JOPES planning which is used to develop OPLANs. While the development of an OPLAN using the JOPES planning process is usually part of the training that takes place during joint exercises, **exercise planning involves all the necessary preparations to structure the exercise and facilitate training**. Most joint exercises are scheduled at an annual exercise planning conference. The results of this conference are promulgated in a CJCS notice. CJCS-

sponsored exercises may be accessed through the Joint Training Information Management Systems via the SIPRNET.

(1) More information about the joint training program can be obtained from Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3500.03A, *Joint Training Manual for the Armed Forces of the United States*. The tasks that must be accomplished during the planning stage for each joint exercise are normally divided between those tasks that must be accomplished prior to the initial planning conference (IPC) and those tasks that should be accomplished **prior to the mid-planning conference (MPC)**, which concludes the planning stage.

(2) IO aspects of an exercise must be concerned with:

(a) **Identifying IO exercise objectives** that are consistent with the overall objectives in scope, purpose, and level of effort.

(b) **Integrating IO tasks and objectives** into the JFC's concept of operations.

(c) **Coordinating IO personnel and assets** to participate as "Blue," "Green," and "Red" forces (if specific force participation has not already been designated by higher authority).

(d) **Identifying personnel with IO expertise** to participate as joint exercise control group and "White Cell" members.

(e) **Determining IO M&S requirements and systems** for the exercise and coordinating their availability and funding.

(f) **Drafting the IO sections of the exercise directive** and supporting plans (to include the exercise control plan).

b. **Exercise Planning Considerations.** When employing IO in exercises, fundamental planning considerations include:

(1) The exercise objectives and how they relate to IO. Planning IO objectives should include a review of the Universal Joint Task List (UJTL), the Joint Mission Essential Task List, and the CJCS' Recommended Training Issues for applicable objectives.

(2) The type, location, and size of exercise, as well as the duration.

(3) Accurate representation of operational target delivery environment.

(4) Lessons learned from previous exercises and operations. The review of lessons learned is an important and cost-effective way to avoid the documented mistakes of previous exercises and operations.

(5) The number and type of IO capabilities and personnel appropriate for the type of exercise and its objectives.

(6) The type of control (free-play, semi-controlled, controlled, or scripted) for IO capabilities necessary to most effectively accomplish the training objectives.

(7) **Defining exercise "play" area(s) in the information environment.** The information environment creates opportunities for remote participation of capabilities and personnel, but also requires concern for inadvertent collateral "damage" or other unintended consequences of exercise information actions not properly "confined." IO capabilities that affect the information environment from CNA or EA exercise activity have the potential to affect or "interact" with the information environment outside the designated exercise area. Exercise planners must evaluate the potential for unintended effects throughout the exercise. Avoiding exercise conflicts with third party Internet or EM spectrum use, involves adherence to guidance provided in training area SOPs, as well as applicable local regulations, laws, treaties, and conventions.

(8) **Need to balance integrated IO training with other training.** The potential for capabilities such as EA and CNA to disrupt exercise play requires that participation of those capabilities be well planned. However, strictly isolated exercise of potentially disruptive capabilities on test ranges and isolated computer networks can lead to false confidence in readiness and inaccurate exercise lessons.

(9) The type of M&S systems to be used as part of the exercise.

(10) The number of experienced IO evaluators required to properly monitor the exercise and assist in developing lessons learned through the after action report (AAR) process.

(11) **Evaluation of possible adverse effects of compromising friendly operations, intelligence capabilities, and methods.** "Real world" OPSEC and other security considerations must be taken into account when planning IO activities. Foreign intelligence organizations often monitor joint exercises to gather information about US capabilities, tactics, techniques, and procedures. IO capabilities and support, participating virtually or from remote locations, should guard against the foreign intelligence collection that targets their communications links with other exercise participants.

c. **Planning Tasks.** The following tasks should be undertaken to ensure that IO is properly integrated into joint exercises when appropriate:

(1) **Developing specific, attainable IO exercise objectives.** The identification and accomplishment of these objectives increase the capability of effectively employing the IO resources and provide the vehicle to evaluate the training of IO personnel. **Objectives must be measurable and compatible with overall exercise constraints.** IO objectives should provide specific direction and should be derived from the UJTL or appropriate OPLAN tasks. General statements of policy and rephrased definitions should be avoided in the development of objectives.

(2) **Providing sufficient opportunity to test the abilities of IO planners to coordinate military information activity, accomplish exercise objectives, and satisfy training requirements.** IO within an exercise must be stimulated through **scenario design, asset participation,** and **scripting of specific events** in the master scenario events list (MSEL).

(3) Designing the IO portion of an exercise scenario in such a way that appropriate assumptions are made about friendly and adversary IO capabilities, baseline perceptions of appropriate individuals and groups, as well as how perceptions may change over the course of the exercise in reaction to all scripted events and exercise play. Baseline perception and IO-related intelligence must be provided in documentation that both Blue and Red forces receive at the start of the exercise (STARTEX). Technical and safety requirements must be coordinated with appropriate range and/or J-6 personnel. IO requirements for M&S must be coordinated. IO experiments during the exercise must be coordinated. MOEs for IO must be identified and documented for exercise evaluators and lessons learned personnel.

(4) Obtaining sufficient IO assets to support training objectives during exercise play. Specific asset availability may be difficult to firmly schedule months before an exercise. Scenario designers should assess the probability of key asset participation and, if necessary, draft backup training objectives and scenario specifics to allow for the loss of exercise assets because of higher priority operational requirements.

(5) Scripting appropriate IO-related events to support training objectives during exercise play. Events scripted to stimulate IO play must be developed as an integrated part of the MSEL. Sufficient IO-related events must be provided to keep participating personnel challenged and achieve training objectives. Where necessary, branch and sequel MSELs must be developed to account for alternative exercise outcomes.

(6) **Creating as realistic an exercise environment as possible.** Realism can be achieved by **using friendly IO capabilities or by employing IO** models and simulations, and incorporating robust IO response cells into the exercise environment. Response cells are especially useful for providing interaction with national-level agencies or departments when conducting strategic influence campaign planning or DSPD. In this regard, there must be an opposing force well-schooled in adversary information techniques in both a conventional and unconventional sense. When US IO planners plan IO actions, they must take into account the presence of realistic opposition forces that will be attempting to anticipate US actions and set conditions for their own effects to work. This interplay also stimulates IO wargaming for information superiority.

(7) **Ensuring adequate manning for IO staff functions and IO evaluation.** IO planners should nominate IO staff billets through the process being used to develop the exercise billet documentation. In addition to the appropriate number of IO billets on the exercise joint staff, IO observer/training billets and IO "white cell" billets may be appropriate, depending on the scale and purpose of the exercise. If IO-related technology or tactics evaluations are to be accomplished during the exercise, additional IO evaluation billets may be necessary.

(8) **Ensuring "real world" OPSEC is considered in the exercise planning.** Coordinate with appropriate authorities to ensure that adequate protection is applied for both simulators and real world systems. These systems should be used at locations and in ways that minimize the success of collection by hostile intelligence systems.

(9) **Coordinating use of simulation to fulfill training objectives.** Force-on-force simulations provide a capability to train battle staffs in the planning, execution, and evaluation of IO employment for any range of scenarios, from a small single-Service counterdrug exercise to a multinational theater campaign.

d. **IO Exercise Planning Flow.** The planning tasks discussed in the previous paragraph must be accomplished within the framework of the three phases of exercise planning culminating in the IPC, MPC, and final planning conference (FPC), respectively. Normally, the IPC occurs approximately eight months prior to the commencement of the exercise. The MPC follows the IPC by about four months. The FPC normally occurs about two months before the exercise.

5. Information Operations Exercise Preparation, Execution, and Post-Exercise Evaluation

The planning stage is only the first of four stages in the life cycle of each joint exercise. The other three stages; preparation, execution, and post-exercise evaluation, also involve tasks and coordination on the part of IO exercise staff personnel.

a. **Preparation Stage.** During the preparation stage, the approved exercise directive and supporting plans are distributed; pre-exercise training is developed and conducted; any exercise specific databases are finalized and tested; and the exercise TPFDD is validated. During this stage, milestones receive a final review and update; operation plans and orders are finalized; simulation gamer augmentees and AAR observer staffing is completed; and the AAR collection management plan is approved. The FPC is conducted to finalize actions required prior to STARTEX. Key actions of the FPC include TPFDL refinement, and the concept of operations and MSEL review as applicable. IO preparations during this period include obtaining necessary clearances and notifications for IO activity (particularly EA and CNA), coordinating implementation of the exercise directive, and accommodating changes in personnel and assets.

b. **Execution Stage.** During the actual conduct of the exercise, personnel responsible for IO should focus on ensuring the IO events in the MSEL occur as planned, the actual IO exercise activities remain focused on the training objectives, and that data/observations supporting the AAR process are properly collected and processed. Prior to the actual STARTEX, it may be necessary or useful to provide structured training on some aspect of IO as a means to achieve one or more of the training objectives. The specifics of such training (who instructs, who attends, where, etc.) should be worked out during the planning and preparation stages of the exercise.

c. **Post-Exercise Evaluation Stage.** This period actually **begins prior to the conclusion of the exercise**. IO activity associated with this stage includes capturing and documenting lessons learned, participating in "hot wash" meetings, and coordinating the redeployment of participants and assets to

parent commands. The form and format for documenting lessons learned can be found in CJCSI 3150.25 Series, *Joint Lessons Learned Program*.

6. Information Operations in Joint Experimentation

a. Conceptualization of the information environment and military activity in it continue to evolve. The joint experimentation (JE) process provides the means to conduct structured analysis of specific IO concepts, concept of operations, doctrine, and capabilities in a controlled environment. This process is crucial to establishing, gauging, and validating proposed IO tactics, techniques, procedures, and capabilities in order to allocate resources efficiently.

b. CJCSI 3180.01, *Joint Requirements Oversight Council (JROC) Programmatic Processes for Joint Experimentation and Joint Resource Change Recommendations*, is the policy document that guides JE. USJFCOM develops the JE campaign plan and coordinates it through Joint Staff J-7, with inputs from the combatant commanders, Services, Joint Staff, OSD, and defense agencies. USJFCOM submits the JE campaign plan for CJCS approval through the JROC process (to include providing briefings to the JROC Joint Review Board).

c. Recommendations resulting from joint IO experiments and other assessments are submitted to the Joint Staff Force Structure, Resource, and Assessment Directorate, in accordance with CJCSI 3180.01 Series, *Joint Requirements Oversight Council (JROC) Programmatic Processes for Joint Experimentation and Joint Resource Change Recommendations*, and other DOD guidance, as required.

APPENDIX A
SUPPLEMENTAL GUIDANCE (PUBLISHED SEPARATELY)

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

Intentionally Blank

MUTUAL SUPPORT WITHIN INFORMATION OPERATIONS CAPABILITIES

	OPSEC	MILDEC	PSYOP	PHYSICAL DESTRUCTION	EW	PHYSICAL SECURITY
OPERATIONS SECURITY (OPSEC) SUPPORTS BY		Concealing competing observables. Degrading general situation information to enhance effect of observables. Limiting information and indicators that could compromise MILDEC operations.	Concealing contradicting indicators while conveying selected information and indicators.	Concealing friendly delivery systems from enemy offensive information operations (IO) until it is too late for the adversary to react. Denying information to the enemy on the success of offensive IO.	Concealing EW units and systems to deny information on extent of electronic attack and electronic warfare support (EA/ES) capabilities.	Concealing essential elements of friendly information (EEFI). Reducing the activities requiring physical security. Hiding tools of physical security thus preventing adversary from gaining access. Information has adequate protection.
MILITARY DECEPTION (MILDEC) SUPPORTS BY	Influencing adversary not to collect against protected units/ activities. Causing adversary to underestimate friendly OPSEC capabilities.		Providing information compatible with PSYOP theme.	Influencing adversary to underestimate friendly physical destruction capabilities. Influencing adversary to defend command and control (C2) elements/systems that friendly forces do not plan to destroy.	Influencing adversary to underestimate friendly EA/ES capabilities.	Masking troop activities requiring safeguards.
PSYCHOLOGICAL OPERATIONS (PSYOP) SUPPORTS BY	Disseminating rules of engagement. Countering propaganda and misinformation. Minimizing resistance and interference by local population.	Creating perceptions and attitudes that MILDEC can exploit. Integrating PSYOP actions with MILDEC. Reinforcing the deception story with information from other sources.		Causing populace to leave targeted areas to reduce collateral damage.	Broadcasting PSYOP products on adversary frequencies. Developing messages for broadcast on other service EW assets.	Targeting adversary audiences to reduce the need for physical security.

Figure B-1. Mutual Support Within Information Operations Capabilities

MUTUAL SUPPORT WITHIN INFORMATION OPERATIONS CAPABILITIES (cont'd)

	OPSEC	MILDEC	PSYOP	PHYSICAL DESTRUCTION	EW	PHYSICAL SECURITY
PHYSICAL ATTACK SUPPORTS BY	Preventing or degrading adversary reconnaissance and surveillance.	Conducting physical attacks as deception events. Degrading adversary capabilities to see, report, and process observables.	Degrading adversary ability to see, report, and process information. Degrading adversary ability to jam PSYOP broadcasts.		Destroying adversary C2 targets. Destroying electronic systems adversary use.	Reducing physical security needs by attacking adversary systems able to penetrate information system (INFOSYS).
ELECTRONIC WARFARE (EW) SUPPORTS BY	Degrading adversary electromagnetic intelligence, surveillance, and reconnaissance (ISR) operations. against protected units and activities Creating barrier of white noise to mask unit maneuvers.	Using EA/ES as deception measures. Degrading adversary capabilities to see, report, and process competing observables. Causing enemy to misinterpret information received by his electronic means.	Degrading adversary's ability to see, report, and process information. Isolating target audience from information.	Providing target acquisition through ES. Destroying or upsetting susceptible assets with EA.		Using electronic protection (EP) to safeguard communications used in protecting facilities.
INFORMATION ASSURANCE (IA) SUPPORTS BY	Ensuring INFOSYS confidentiality.	Providing INFOSYS assets for conducting MILDEC operations.	Ensuring availability of INFOSYS for PSYOP.	Ensuring INFOSYS are available for physical destruction tasks.	Ensuring EW assets are available.	Providing for INFOSYS authentication.
COMPUTER NETWORK ATTACK (CNA) SUPPORTS BY	Attacking enemy computers before they can detect our EEFI.	Providing the deception story through computers.	Another means of providing the PSYOP theme.	Nonlethal attack of selected targets, which allows lethal attacks on other targets.	Used with EA.	Conducting risk assessment to determine consequence of 2d and 3d order CNA effects.
COMPUTER NETWORK DEFENSE (CND) SUPPORTS BY	Detecting enemy attempts to acquire information.	Protecting the MILDEC plan resident inside computers.	Preventing the compromise of PSYOP message before release.	Protecting fire support C2 systems.	Used in conjunction with EP.	Erect firewalls to protect intrusion into networks.

Figure B-1. Mutual Support Within Information Operations Capabilities (cont'd)

MUTUAL SUPPORT WITHIN INFORMATION OPERATIONS CAPABILITIES (cont'd)

	OPSEC	MILDEC	PSYOP	PHYSICAL DESTRUCTION	EW	PHYSICAL SECURITY
PHYSICAL SECURITY SUPPORTS BY	Protecting operation plans and operation orders.	Restricting access by level of security and number of personnel.	Ensuring products do not contain classified information	Safeguarding availablity of INFOSYS to use in physical destruction.	Safeguarding equipment used in EW.	
COUNTER-INTELLIGENCE (CI) SUPPORTS BY	Countering foreign human intelligence (HUMINT) operations.	Countering foreign HUMINT operations. Identifying threat ISR capabilities.	Conducting countersignal operations to allow broadcast of PSYOP messages	None	Providing electronic countermeasures.	Countering foreign HUMINT operations.

	IA	CI	CNA	CND
OPSEC SUPPORTS BY	Concealing physical and electronic INFOSYS locations.	Ensuring EEFI are concealed from enemy collection assets.	Concealing CNA capabilities.	Denying enemy knowledge about CND capabilities.
MILDEC SUPPORTS BY	Overloading adversary intelligence and analysis capabilities. Protecting and defending friendly INFOSYS.	Giving the adversary a cover story so his intelligence system collects irrelevant information.	Providing MILDEC targets and deception stories to enhance CNA.	Causing enemy to believe our CND is greater than it actually is. Causing enemy to believe all CND tools are in place.
PSYOP SUPPORTS BY	Enhancing the ability of IA in the minds of the enemy.	Providing messages in enemy decision maker's mind that can be revealed by CI to determine enemy true intentions.	Convincing enemy not to do something by describing effects of a CNA if they take undesirable actions.	Providing information about non-military threat to computers in the area of operations.
PHYSICAL ATTACK SUPPORTS BY	Attacking adversary systems capable of influencing friendly INFOSYS availability and integrity.	Destroying appropriately nominated adversary collection assets.	Supplementing CNA by destroying or degrading hard targets.	Destroying or degrading enemy CNA facilities before they attack friendly computers.
EW SUPPORTS BY	Using EP to protect equipment.	None	Supplementing CNA with EA.	Using EP to protect personnel, facilities, and equipment.

Figure B-1. Mutual Support Within Information Operations Capabilities (cont'd)

MUTUAL SUPPORT WITHIN INFORMATION OPERATIONS CAPABILITIES (cont'd)

	IA	CI	CNA	CND
IA SUPPORTS BY		Ensuring INFOSYS are available to conduct CI.	Ensuring links with higher headquarters to pass CNA requests.	Taking actions to ensure availability, integrity, authentication, confidentiality, and nonrepudiation of computers.
CNA SUPPORTS BY	Attacking enemy computers before enemy attacks friendly computers.	Exploiting enemy intelligence collection.		Attacking enemy ability to attack friendly computers.
CND SUPPORTS BY	Supporting IA of information passed via computer networks.	Detecting, identifying, and assessing enemy collection efforts against computers.	Protecting CNA weapons from enemy detection.	
PHYSICAL SECURITY SUPPORTS BY	Safeguarding INFOSYS by implementing security procedures.	Safeguarding personnel, and preventing unauthorized access to equipment, installations, materiel, and documents.	Safeguarding INFOSYS from sabotage, espionage, damage, or theft.	Determining applicable risk and threat levels.
CI SUPPORTS BY	At certain echelons, helping ensure information integrity.		Confirming results of CNA.	Detecting, identifying, assessing, countering, and neutralizing enemy intelligence collection.

Figure B-1. Mutual Support Within Information Operations Capabilities (cont'd)

POTENTIAL CONFLICTS WITHIN THE CAPABILITIES OF INFORMATION OPERATIONS

	OPSEC	MILDEC	PSYOP	PHYSICAL DESTRUCTION	EW	PHYSICAL SECURITY
OPERATIONS SECURITY (OPSEC) CAN CONFLICT BY		Limiting information that can be revealed to enhance deception story credibility.	Limiting information that can be revealed to develop PSYOP themes.	Limiting information that can be revealed to enemy to develop targets.	Electronic protection (EP) and OPSEC may have different goals.	Should be no conflict.
MILITARY DECEPTION (MILDEC) CAN CONFLICT BY	Revealing information OPSEC normally seeks to conceal.		Limiting PSYOP theme selection. Limiting information that can be revealed to develop PSYOP themes.	Limiting targeting to allow survival and conduct of critical adversary command and control (C2) functions.	Limiting electronic attack (EA) targeting of adversary information systems (INFOSYS) to allow survival and conduct of critical adversary C2 functions.	Negating the deception story by physical security preventing our transmitting a realistic deception story.
PSYCHOLOGICAL OPERATIONS (PSYOP) CAN CONFLICT BY	Revealing information OPSEC normally seeks to conceal.	Limiting deception story selection if deception story contains untruths.		Limiting targeting of adversary C2 infrastructure to allow conveying of PSYOP themes.	Limiting EA against adversary communications frequencies to allow PSYOP themes to be conveyed.	Should be no conflict.
PHYSICAL ATTACK CAN CONFLICT BY	Causing firing systems to reveal their locations.	Limiting selection of deception means by denying or degrading elements of adversary C2 infrastructure necessary to process deception story.	Limiting means available to convey PSYOP themes by denying or degrading adversary C2 systems.		Limiting opportunities for communications intrusion by denying or degrading elements of adversary INFOSYS.	If need-to-know considerations limit access to targeting data.
ELECTRONIC WARFARE (EW) CAN CONFLICT BY	Revealing EW assets prematurely.	Limiting selection of deception measures by denying or degrading use of adversary C2 systems.	Reducing frequencies available to convey PSYOP themes.	Limiting targeting of adversary C2 systems.		Revealing what physical security is trying to protect (EA). EP should not conflict.

Figure B-2. Potential Conflicts Within the Capabilities of Information Operations

POTENTIAL CONFLICTS WITHIN THE CAPABILITIES OF INFORMATION OPERATIONS (cont'd)

	OPSEC	MILDEC	PSYOP	PHYSICAL DESTRUCTION	EW	PHYSICAL SECURITY
INFORMATION ASSURANCE (IA) CAN CONFLICT BY	Should be no conflict.	Reinforcing the deception story	Should be no conflict.	Should be no conflict.	EP and IA must be deconflicted.	Should be no conflict.
COMPUTER NETWORK ATTACK (CNA) CAN CONFLICT BY	Attack selected on enemy targets may provide information on friendly activities.	May result in attacking wrong target if coordination not made with MILDEC	Preventing the enemy from receiving the PSYOP message.	Attacking same target with nonlethal and lethal weapons wastes both time and ammunition.	Need to deconflict which systems attack which targets.	Revealing CNA source that should be protected.
COMPUTER NETWORK DEFENSE (CND) CAN CONFLICT BY	Should be no conflict.	Reinforcing the deception story	Should be no conflict.	Should be no conflict.	Should be no conflict.	Should be no conflict.
COUNTER-INTELLIGENCE (CI) CAN CONFLICT BY	Should be no conflict.	Should be no conflict	Should be no conflict.	Killing sources.	Electronic warfare support may be needed for other activities.	Should be no conflict.

	IA	CI	CNA	CND
OPSEC CAN CONFLICT BY	Should be no conflict.	Should be no conflict.	Should be no conflict.	Should be no conflict.
MILDEC CAN CONFLICT BY	Presenting data the enemy will believe versus assuring data is not revealing to enemy.	Giving the adversary a cover story that inadvertently supports his collection plan.	Should be no conflict.	Should be no conflict.
PSYOP CAN CONFLICT BY	Should be no conflict.	Should be no conflict.	Should be no conflict.	Should be no conflict.

Figure B-2. Potential Conflicts Within the Capabilities of Information Operations (cont'd)

POTENTIAL CONFLICTS WITHIN THE CAPABILITIES OF INFORMATION OPERATIONS (cont'd)

	IA	CI	CNA	CND
PHYSICAL ATTACK CAN CONFLICT BY	Attacking incorrect adversary systems capable of influencing friendly INFOSYS availablity and integrity.	Destroying insufficient number of adversary collection assets.	Should be no conflict.	Should be no conflict.
EW CAN CONFLICT BY	Should be no conflict.	Should be no conflict.	Should be no conflict.	Should be no conflict.
IA CAN CONFLICT BY		Having insufficient INFOSYS available to conduct CI.	Not having available links with higher headquarters to pass CNA requests.	Should be no conflict.
CNA CAN CONFLICT BY	Should be no conflict.	Attacking enemy computers before exploiting hostile intelligence collection efforts.		Should be no conflict.
CND CAN CONFLICT BY	Should be no conflict.	Should be no conflict.	Should be no conflict.	
PHYSICAL SECURITY CAN CONFLICT BY	Should be no conflict.	Should be no conflict.	Should be no conflict.	Should be no conflict.
CI CAN CONFLICT BY	Ineffective CI can negate information integrity.		Should be no conflict.	CI revealing how networks are protected.

Figure B-2. Potential Conflicts Within the Capabilities of Information Operations (cont'd)

SUPPORT ROLES OF INFORMATION OPERATIONS, CIVIL-MILITARY OPERATIONS, PUBLIC AFFAIRS, DEFENSE SUPPORT TO PUBLIC DIPLOMACY, AND COMBAT CAMERA

	INFORMATION OPERATIONS	CIVIL MILITARY OPERATIONS	PUBLIC AFFAIRS	DEFENSE SUPPORT TO PUBLIC DIPLOMACY	COMBAT CAMERA
INFORMATION OPERATIONS (IO) SUPPORTED BY		Influencing/informing populace of CMO activities and support. Neutralizing misinformation and hostile propaganda directed against civil authorities. Controlling electromagnetic spectrum for legitimate purposes.	Conducting counter-propaganda and protection from misinformation/rumor. Developing essential elements of friendly information (EEFI) to preclude inadvertent public disclosure. Synchronizing psychological operations (PSYOP) and operations security (OPSEC) with PA strategy.	Ensuring accuracy of information. Maintaining relevance of information. Timeliness of information. Usability of information. Completeness of information. Security of information.	Coordinating guidance to COMCAM teams with commander's information/objectives. Assisting in expeditious transmission of critical COMCAM images.
CIVIL MILITARY OPERATIONS (CMO) SUPPORTS BY	Providing information to support friendly knowledge of information environment. Synchronizing communications media and assets and message with other IO capabilities. Coordinating command and control target sets with targeting cell. Establishing and maintaining liaison or dialogue with indigenous personnel and nongovernmental organizations (NGOs). Supporting PSYOP with feedback on PSYOP themes. Providing news and information to the local people.		Providing information on civil-military operations center activities to support public affairs (PA) strategy. Synchronizing information communications media and message. Identifying, coordinating, and integrating media, public information, and host-nation support.	Providing information to inform interagency elements on local information environment. Synchronizing communications media and messages with other IO capabilities. Establishing and maintaining liaison or dialogue with indigenous personnel and NGOs. Supporting DPSD with feedback on strategic communications themes.	Using COMCAM capabilities to record priority civic action projects. Synchronizing imagery assignments with COMCAM team leader.

Figure B-3. Support Roles of Information Operations, Civil-Military Operations, Public Affairs, Defense Support to Public Diplomacy, and Combat Camera

SUPPORT ROLES OF INFORMATION OPERATIONS, CIVIL-MILITARY OPERATIONS, PUBLIC AFFAIRS, DEFENSE SUPPORT TO PUBLIC DIPLOMACY, AND COMBAT CAMERA (cont'd)

	INFORMATION OPERATIONS	CIVIL MILITARY OPERATIONS	PUBLIC AFFAIRS	DEFENSE SUPPORT TO PUBLIC DIPLOMACY	COMBAT CAMERA
PUBLIC AFFAIRS (PA) SUPPORTED BY	Developing information products to protect soldiers against the effects of misinformation or disinformation. Coordinating with IO planners to ensure a consistent message and maintain OPSEC. Supporting counterpropaganda by countering misinformation. Providing assessment of effects of media coverage to OPSEC planners. Providing assessment of essential nonmedia coverage of deception story.	Producing accurate, timely, and balanced information for the public. Coordinating with civil affairs specialists to verify facts and validity of information.		Developing information products to protect US actions consistent with strategic communications themes and objectives. Coordinating with interagency planners to ensure a consistent message. Providing assessment of media coverage.	Managing release of key images through PA channels. Coordinating for COMCAM coverage and access to key events and operations.
DEFENSE SUPPORT TO PUBLIC DIPLOMACY (DSPD) SUPPORTS BY	Providing a link to interagency for coordination and guidance on strategic communications themes and activities.	Providing a link to interagency for coordination and guidance on strategic communications themes and activities.	Providing a link to interagency for coordination and guidance on strategic communications themes and activities.		Providing a link to interagency for coordination and guidance on strategic communications themes and activities.
COMBAT CAMERA (COMCAM) SUPPORTS BY	Providing responsive imagery coverage of events in the operational area.	Providing responsive imagery coverage of events in the operational area.	Providing responsive imagery coverage of events in the operational area.	Providing responsive imagery coverage of events in the operational area.	

Figure B-3. Support Roles of Information Operations, Civil-Military Operations, Public Affairs, Defense Support to Public Diplomacy, and Combat Camera (cont'd)

Intentionally Blank

APPENDIX C
COMMUNICATIONS SYSTEM SUPPORT TO INFORMATION OPERATIONS

1. Introduction

Joint communications systems support the warfighting commander across the range of military operations. DOD communications systems are designed, acquired, and linked according to principles that provide for flexible, adaptable use in a wide variety of applications. Normally, IO is planned, directed, and supported on the resident command or organizational communications systems which support other communications requirements. Personnel responsible for IO or IO support at each DOD component use communications systems available to other command personnel in compliance with appropriate IA, information management, and administrative policies. The IO cell chief, or other designated person, provides communications system support requirements through staff procedures established locally. Whether core capability staff sections submit their communications support requirements through the IO cell chief is command specific. At each command, IO communications requirements are prioritized with other unit or organizational communications requirements. During operational planning, IO and capability-specific frequency and bandwidth requirements are negotiated as part of the JOPES or other designated planning process.

For more discussion on communications system support, see JP 6-0, Communications System Support to Joint Operations.

2. Joint Force Communications System Directorate

a. The J-6 is responsible to the JFC for providing the communications system to support reliable, timely information flow in support of unified action. The operational arm of the J-6 is the JNCC. JNCCs play a vital role in IO, particularly in the IA process, where they provide communications and network connectivity throughout the chain of command. The J-6 establishes a JNCC to manage all communications systems deployed in the operational area. The JNCC requires timely support from subordinate command's communications control centers to direct network operations (NETOPS) and retain situational awareness of force networks.

b. The JNCC serves as the single control agency for the management of the joint communications system in an operational area. The JFC may task subordinate Service or component commanders to provide personnel augmentation to the J-6 to ensure the appropriate subject matter expertise exists within the JNCC. Combatant commanders and component commanders should designate a single office within their communications staffs to coordinate with the J-6.

c. The JNCC may incorporate the use of a joint network management system, which may include the joint defense infrastructure control system. These systems play a high-level role in the network planning, monitoring, and control of the system, illustrating the network common operational picture used in combat operations.

3. Communications System Directorate Responsibilities

a. Exercises staff supervision of all communications system assets. Publishes communications system plans, annexes, and operating instructions to support the assigned mission, furnishing direction to subordinate commands regarding provision of communications system assets required to support the JFC. This may include assigning primary responsibility for communications to a subordinate or component command. The J-6 also assigns responsibility for lateral communications between subordinate commands.

b. Provide overall management of the communications system supporting the JFC.

c. Review and coordinate communications system plans prepared by subordinate commands.

d. Upon requesting CJCS-controlled transportable assets, including JCSE assets, in accordance with CJCSI 6110.01A, *CJCS-Controlled Communications Assets*, and other established procedures, exercises staff supervision when deployed to the operational area.

e. Ensure interoperability of the joint communications system.

4. Joint Network Operations Control Center Responsibilities

a. Exercise technical management over communications control centers belonging to deployed components and subordinate commands.

b. Serves as the single control agency for management of the joint communications networks and infrastructure.

c. Perform planning, execution, technical, and management functions.

d. Develop/disseminate standards/procedures and collect/present communications system management statistical data.

For more discussion on NETOPS and JNCC see JP 6-0, Communications System Support to Joint Operations.

APPENDIX D
REFERENCES

The development of JP 3-13 is based upon the following primary references.

1. Executive Branch Documents

a. *National Security Strategy.*

b. *Unified Command Plan FY 04* (through Chg 2).

c. Executive Order 12333, *United States Intelligence Activities*.

2. Department of State Documents

Department of State Publication 9434, *Treaties In Force*.

3. Department of Defense Documents

a. *IO Roadmap.*

b. DODD 3222.4, *Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures.*

c. DODD S-3321.1, *Overt Psychological Operations Conducted by the Military Services in Peacetime in Contingencies Short of Declared War.*

d. DODD 3600.1, *Information Operations (IO)* (SD 106 Formal Coordination Draft).

e. DODD 5122.5, *Assistant Secretary of Defense for Public Affairs (ASD(PA)).*

f. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*.

g. DODD 5205.2, *DOD Operations Security (OPSEC) Program.*

h. DODD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*.

i. DODD 5240.2, *DOD Counterintelligence (CI)*.

j. DODD 8500.1, *Information Assurance (IA).*

k. DODD O-8530.1, *Computer Network Defense (CND*).

l. DODI O-3600.02, *Information Operations (IO) Security Classification Guidance (U).*

m. DODI 3608.11, *Information Operations Career Force*.

n. DODI 5240.4, *Reporting of Counterintelligence and Criminal Violations.*

o. DODI 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs.*

p. DODI 5240.10, *Counterintelligence Support to the Combatant Commands and the Defense Agencies.*

q. DODI 8500.2, *Information Assurance (IA) Implementation.*

r. DODI O-8530.2, *Support to Computer Network Defense (CND*).

s. *National Military Strategy* (2004).

4. Joint Policy, Doctrine, and Other Publications

a. CJCSI 1800.01B, *Officer Professional Military Education Policy.*

b. CJCSI 3110.05C, *Joint Psychological Operations Supplement to the Joint Strategic Capabilities Plan FY 2002.*

c. CJCSI 3113.01, *Responsibilities for the Management and Review of Theater Engagement Plans.*

d. CJCSI 3141.01B, *Responsibilities for the Management and Review of Operation Plans.*

e. CJCSI 3150.25B, *Joint Lessons Learned Program.*

f. CJCSI 3170.01E, *Joint Capabilities Integration and Development System.*

g. CJCSI 3180.01, *Joint Requirements Oversight Council (JROC) Programmatic Processes for Joint Experimentation and Joint Resource Change Recommendations.*

h. CJCSI 3210.01A, *Joint Information Operations Policy.*

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

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

k. CJCSI 3213.01B, *Joint Operations Security.*

l. CJCSI 3401.03A, *Information Assurance (IA) and Computer Network Defense (CND) Joint Quarterly Readiness Review (JQRR) Metrics.*

m. CJCSI 6510.01D, *Information Assurance (IA) and Computer Network Defense (CND).*

n. CJCSM 3113.01A, *Theater Engagement Planning.*

o. CJCSM 3122.01, *Joint Operation Planning and Execution System (JOPES) Volume I (Planning Policies and Procedures).*

p. CJCSM 3122.02C, *Joint Operation Planning and Execution System (JOPES) Volume II (Crisis Action Time-Phased Force and Deployment Data Development and Deployment Execution).*

q. CJCSM 3122.03A, *Joint Operation Planning and Execution System Volume II, Planning Formats and Guidance.*

r. CJCSM 3122.04A, *Joint Operation Planning and Execution System Volume II – Supplemental Planning Formats and Guidance.*

s. CJCSM 3141.01A, *Procedures for the Review of Operation Plans*.

t. CJCSM 3500.03A, *Joint Training Manual for the Armed Forces of the United States.*

u. CJCSM 3500.04D, *Universal Joint Task List (UJTL).*

v. CJCSM 3500.04C, Series 01, *Classified Supplement To The Universal Joint Task List (UJTL)*.

w. CJCSM 6510.01, *Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND).*

x. JP 0-2, *Unified Action Armed Forces (UNAAF).*

y. JP 1-04, *Joint Tactics, Techniques, and Procedures for Legal Support to Military Operations* (Pre Approval Draft).

z. JP 2-0, *Doctrine for Intelligence Support to Joint Operations*.

aa. JP 2-01, *Joint and National Intelligence Support to Military Operations.*

bb. JP 2-01.2, *Counterintelligence and Human Intelligence Support to Joint Operations.*

cc. JP 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.*

dd. JP 2-03, *Geospatial Intelligence (GEOINT) Support to Joint Operations*.

ee. JP 3-0, *Joint Operations.*

ff. JP 3-01.4, *JTTP for Joint Suppression of Enemy Air Defenses (J-SEAD).*

gg. JP 3-03, *Doctrine for Joint Interdiction Operations.*

hh. JP 3-05.2, *Joint Tactics, Techniques, and Procedures for Special Operations Targeting and Mission Planning.*

ii. JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol. I.*

jj. JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol. II.*

kk. JP 3-09, *Joint Fires.*

ll. JP 3-10, *Joint Security Operations in the Theater.*

mm. JP 3-14, *Joint Doctrine for Space Operations.*

nn. JP 3-30, *Command and Control for Joint Air Operations.*

oo. JP 3-31, *Command and Control for Joint Land Operations.*

pp. JP 3-51, *Electronic Warfare.*

qq. JP 3-53, *Joint Doctrine for Psychological Operations.*

rr. JP 3-54, *Operations Security.*

ss. JP 3-57, *Joint Doctrine for Civil-Military Operations.*

tt. JP 3-58, *Military Deception.*

uu. JP 3-60, *Targeting.*

vv. JP 3-61, *Public Affairs.*

ww. JP 5-0, *Joint Operation Planning*.

xx. JP 5-00.2 *Joint Task Force Planning Guidance and Procedures.*

yy. JP 6-0, *Communications System Support to Joint Operations.*

zz. *Joint Forces Staff College IO Planning Handbook (2003).*

aaa. *Standing Joint Task Force Standard Operating Procedures (Draft).*

bbb. *USJFCOM Standard Operation Procedure & Tactics, Techniques, and Procedures for the Standing Joint Force Headquarters (Core Element)*, 14 July 2004.

ccc. *USJFCOM Joint Warfighting Center Pamphlet 3: Doctrinal Implications of the Standing Joint Force Headquarters (SJFHQ)*, 16 June 2004.

ddd. *The Privacy Act, Title 5 US Code Section 552a.*

5. Multi-Service and Service Publications

a. Field Manual 3-13 *Information Operations: Doctrine, Tactics, Techniques, and Procedures.*

b. Naval Warfare Publication 3-13, *Navy Information Operations.*

c. Air Force Doctrine Document 2-5, *Information Operations.*

d. *United States Air Force Concept of Operations for Information Operations.*

e. *A Concept for Information Operations* (USMC document).

f. *Multi-Service Tactics, Techniques, and Procedures for Joint Combat Camera* of March 2003.

Intentionally Blank

APPENDIX E
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

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

2. Authorship

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

3. Supersession

This publication supersedes JP 3-13, 9 October 1998, *Joint Doctrine for Information Operations* and JP 3-13.1, 7 February 1996, *Joint Doctrine for Command and Control Warfare (C2W)*.

4. Change Recommendations

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

TO: JOINT STAFF WASHINGTON DC//J3-DDGO//
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//
CDRUSJFCOM SUFFOLK VA//DOC GP//

Routine changes should be submitted electronically to Commander, Joint Warfighting Center, Doctrine and Education Group and info the Lead Agent and the Director for Operational Plans and Joint Force Development J-7/JEDD via the CJCS JEL at http://www.dtic.mil/doctrine.

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 Joint Staff/J-7 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

5. Distribution of Printed Publications

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

b. Individuals and agencies outside the combatant commands, Services, Joint Staff, and combat support agencies are authorized to receive only approved joint publications and joint test publications. 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, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 15 November 1999, *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: Commander (Attn: Publications)
814 Radford Blvd, Suite 20321
Albany, GA 31704-0321

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

Commander
USJFCOM JWFC Code JW2102
Doctrine and Education Group (Publication Distribution)
116 Lake View Parkway
Suffolk, VA 23435-2697

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

6. Distribution of Electronic Publications

a. The Joint Staff will not print copies of electronic joint publications for distribution. Electronic versions are available at www.dtic.mil/doctrine (NIPRNET), or http://nmcc20a.nmcc.smil.mil/dj9j7ead/doctrine/ (SIPRNET).

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

Intentionally Blank

GLOSSARY
PART I — ABBREVIATIONS AND ACRONYMS

AAR	after action report
AOR	area of responsibility
BDA	battle damage assessment
C2	command and control
CA	civil affairs
CDRUSSTRATCOM	Commander, United States Strategic Command
CE	core element
CI	counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
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
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
COA	course of action
COMCAM	combat camera
COMSEC	communications security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOS	Department of State
DSPD	defense support to public diplomacy
EA	electronic attack (previously ECM)
EM	electromagnetic
EP	electronic protection
ES	electronic warfare support (previously ESM)
EW	electronic warfare
EWCC	electronic warfare coordination cell
FPC	final planning conference
GEOINT	geospatial intelligence
HQ	headquarters

IA	information assurance
IC	intelligence community
IO	information operations
IPB	intelligence preparation of the battlespace
IPC	initial planning conference
IT	information technology
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-6	communications system directorate of a joint staff
J-7	Operational Plans and Joint Force Development Directorate, Joint Staff
JA	judge advocate
JCMA	joint communications security (COMSEC) monitoring activity
JCSE	joint communications support element
JE	joint experimentation
JFC	joint force commander
JIPB	joint intelligence preparation of the battlespace
JNCC	joint network operations control center
JOC	joint operations center
JOPES	Joint Operation Planning and Execution System
JP	joint publication
JPO-STC	Joint Program Office for Special Technology Countermeasures
JPOTF	joint psychological operations task force
JRFL	joint restricted frequency list
JROC	Joint Requirement Oversight Council
JSC	Joint Spectrum Center
JTCB	joint targeting coordination board
JTF	joint task force
JWAC	joint warfare analysis center
LOAC	law of armed conflict
M&S	modeling and simulation
MASINT	measurement and signature intelligence
MILDEC	military deception
MNF	multinational force
MNFC	multinational force commander
MOE	measure of effectiveness
MOP	measure of performance
MPC	mid-planning conference
MSEL	master scenario events list

NDP	national disclosure policy
NETOPS	network operations
NGA	National Geospatial-Intelligence Agency
NGO	nongovernmental organization
NSA	National Security Agency
OPLAN	operation plan
OPSEC	operations security
OSD	Office of the Secretary of Defense
PA	public affairs
PD	public diplomacy
PIR	priority intelligence requirement
POAT	psychological operations assessment team
PSYOP	psychological operations
RFI	request for information
SecDef	Secretary of Defense
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SJFHQ	standing joint force headquarters
SME	subject matter expert
SOF	special operations forces
SOP	standing operating procedure
STARTEX	start of the exercise
STO	special technical operations
TA	target audience
TPFDD	time-phased force and deployment data
TPFDL	time-phased force and deployment list
TSCP	theater security cooperation plan
UJTL	Universal Joint Task List
USG	United States Government
USJFCOM	United States Joint Forces Command
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command

air tasking order. A method used to task and disseminate to components, subordinate units, and command and control agencies projected sorties, capabilities and/or forces to targets and specific missions. Normally provides specific instructions to include call signs, targets, controlling agencies, etc., as well as general instructions. Also called ATO. (JP 1-02)

battlespace. The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest. (JP 1-02)

campaign plan. A plan for a series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space. (JP 1-02)

civil-military operations. The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. Also called CMO. (JP 1-02)

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

combatant command (command authority). Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally, this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ

commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). Also called COCOM. (JP 1-02)

combat camera. The acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services. Also called COMCAM. (JP 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. (JP 1-02)

command and control warfare. None. (Approved for removal from the next edition of JP 1-02.)

command relationships. The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command; defined further as combatant command (command authority), operational control, tactical control, or support. (JP 1-02)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications security includes: cryptosecurity, transmission security, emission security, and physical security. Also called COMSEC. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 6-0.)

computer intrusion. An incident of unauthorized access to data or an automated information system. (JP 1-02)

computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

computer network defense. Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. Also called CND. (This term and its definition

modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

computer network exploitation. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE. (Approved for inclusion in the next edition of JP 1-02.)

computer network operations. Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO. (Approved for inclusion in the next edition of JP 1-02.)

concept of operations. A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations. The concept of operations frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Also called commander's concept or CONOPS. (JP 1-02)

coordinating authority. A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more Military Departments, two or more joint force components, or two or more forces of the same Service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations. (JP 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. (JP 1-02)

cryptosecurity. The component of communications security that results from the provision of technically sound cryptosystems and their proper use. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 6-0.)

cyberspace. The notional environment in which digitized information is communicated over computer networks. (JP 1-02)

data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any

representations such as characters or analog quantities to which meaning is or might be assigned. (JP 1-02)

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

defense support to public diplomacy. Those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government. Also called DSPD. (Approved for inclusion in the next edition of JP 1-02.)

defensive information operations. None. (Approved for removal from the next edition of JP 1-02.)

directed energy. An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. Also called DE. (JP 1-02)

electromagnetic spectrum. The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. See also electronic warfare. (JP 1-02)

electromagnetic spectrum management. Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 6-0.)

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 energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under

direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. See also directed energy; electromagnetic spectrum. (JP 1-02)

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. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 6-0.)

fires. Actions using lethal and nonlethal weapons to produce a specific effect on a target. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-0.)

fire support. Fires that directly support land, maritime, amphibious, and special operations forces to engage enemy forces, combat formations, and facilities in pursuit of tactical and operational objectives. (JP 1-02)

fire support coordination. The planning and executing of fire so that targets are adequately covered by a suitable weapon or group of weapons. (JP 1-02)

geospatial intelligence. The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically reference activities on the Earth. Also called GEOINT. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 2-03.)

Global Information Grid. The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services and National Security Systems. Also called GIG. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 6-0.)

human factors. In information operations, the psychological, cultural, behavioral, and other human attributes that influence decision making, the flow of information, and the interpretation of information by individuals or groups at any level in a state or organization. (Approved for inclusion in the next edition of JP 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. (JP 1-02)

information assurance. Measures 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 modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information operations. The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called IO. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information security. The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Also called INFOSEC. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information system. The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information warfare. None. (Approved for removal from the next edition of JP 1-02.)

integration. 2. The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 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 database for each potential

area in which a unit may be required to operate. The database 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. (JP 1-02)

interagency coordination. The coordination that occurs between agencies of the US Government, including the Department of Defense, for the purpose of accomplishing an objective. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-08.)

joint fires. Fires produced during the employment of forces from two or more components in coordinated action toward a common objective. See also fires. (JP 1-02)

joint fire support. Joint fires that assist air, land, maritime, amphibious, and special operations forces to move, maneuver, and control territory, populations, airspace, and key waters. See also fire support; joint fires. (JP 1-02)

joint targeting coordination board. A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance and priorities, and refining the joint integrated prioritized target list. The board is normally comprised of representatives from the joint force staff, all components, and if required, component subordinate units. Also called JTCB. (JP 1-02)

leveraging. None. (Approved for removal from the next edition of JP 1-02.)

military deception. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces mission. Also called MILDEC. See also deception. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-58.)

offensive information operations. None. (Approved for removal from the next edition of JP 1-02.)

operation. 1. A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission. 2. The process of carrying on combat, including movement, supply, attack, defense, and maneuvers needed to gain the objectives of any battle or campaign. (JP 1-02)

operational art. The employment of military forces to attain strategic and/or operational objectives through the design, organization, integration, and conduct of strategies, campaigns, major operations, and battles. Operational art translates the joint force commander's strategy into operational design and, ultimately, tactical action, by integrating the key activities at all levels of war. (JP 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 that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 1-02)

physical security. 1. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. 2. In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. See also communications security. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 6-0.)

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. (JP 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. (JP 1-02)

public diplomacy. Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. (JP 1-02)

reachback. The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02)

space. A medium like the land, sea, and air within which military activities shall be conducted to achieve US national security objectives. (JP 1-02)

space control. Combat, combat support, and combat service support operations to ensure freedom of action in space for the United States and its allies and, when directed, deny an adversary freedom of action in space. The space control mission area includes: surveillance of space; protection of US and friendly space systems; prevention of an adversary's ability to use space systems and services for purposes hostile to US national security interests; negation

of space systems and services used for purposes hostile to US national security interests; and directly supporting battle management, command, control, communications, and intelligence. (JP 1-02)

strategic communication. Focused United States Government (USG) efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power. (Approved for inclusion in the next edition of JP 1-02.)

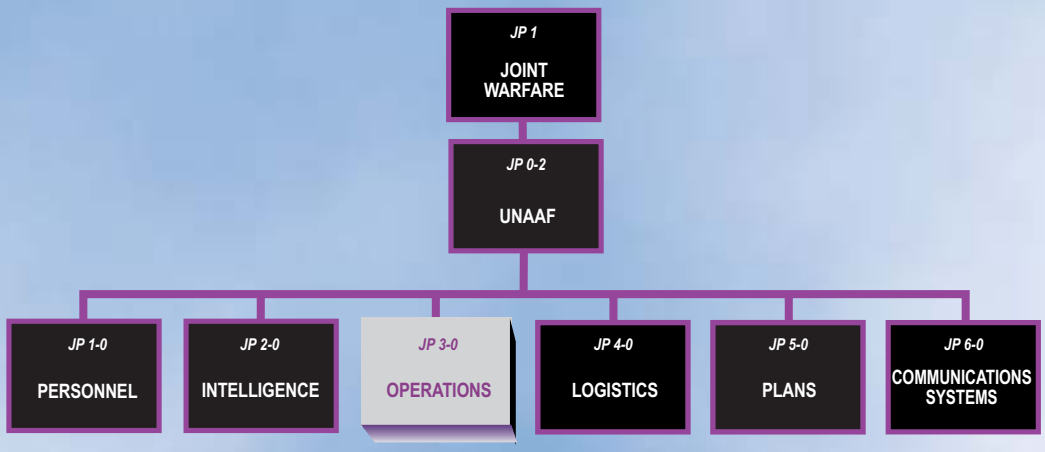
synchronization. 1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. (JP 1-02)

target audience. An individual or group selected for influence. Also called TA. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

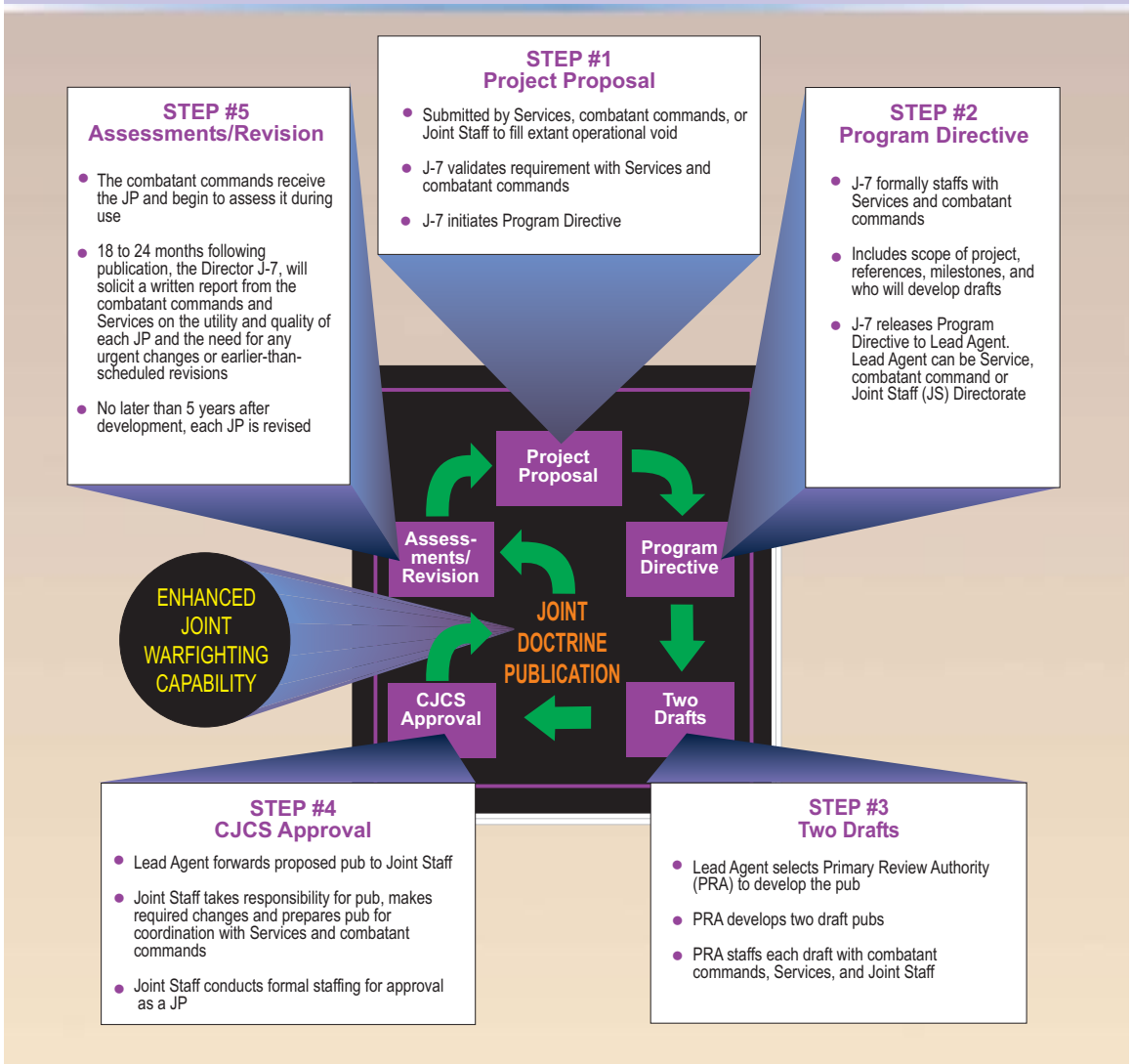
transmission security. The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 6-0.)

vulnerability analysis. None. (Approval for removal from the next edition of JP 1-02.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine is organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-13** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:



JOINT
CHIEFS OF STAFF