Joint Publication 3-13

Joint Doctrine for Information Operations

Second Draft

14 December 2004

PREFACE

1. Scope

This publication addresses information operations ~~(IO)~~ planning and execution in support of joint~~,~~ and multinational~~,~~ operations and interagency ~~efforts~~ coordination across the range of military operations. ~~This edition is a complete revision of the previous edition of Joint Pub 3-13, *Joint Doctrine for Information 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:

T. J. KEATING
Vice Admiral, USN
Director, Joint Staff

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

- **Summary of Changes to be provided**
-
-
-
-
-

Intentionally Blank

TABLE OF CONTENTS

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

-
-
-
-

To be completed at Final Coordination.

Intentionally Blank

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

1. Introduction

Information operations (IO) are integral to successful military operations. A key goal of IO is to achieve and maintain information superiority for the United States and its allies. ~~Information operations (~~IO~~)~~ are ~~defined~~ described as "the integrated employment of the core capabilities of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp ~~adversarial~~ adversary human and automated decision making while protecting our own." The purpose of this doctrine is to ~~expand on that definition in the~~ provide details necessary for joint force commanders (JFCs~~),~~ ~~joint warfighters,~~ and those that support them to understand, plan, execute, train to, and support IO ~~as a part of joint operations~~. ~~The majority of this publication deals with the specifics necessary to plan and execute IO in joint operations. However, it is first necessary to establish the conceptual context for IO from a joint doctrine perspective. The next two sections discuss the information dimension and military operations in relation to that dimension. The fourth section defines and discusses the concept of information fire. These three sections are necessary to place IO in the context of other informational activities, explain IO's value in military operations, and, perhaps most importantly, clarify what IO is not. The fifth section discusses the principals of IO on which DOD policy and doctrine are based. The final section of the chapter reviews the DOD policy framework for IO.~~

2. The Information ~~Dimension~~Environment

a. ~~The information environment is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information, and information itself. Individual perceptions of the information environment are affected by many factors, including culture, language, and education. For simplicity's sake, in the context of this publication, the terms "data" and "information" are termed "information."~~ The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. From an operational perspective, decision makers utilize the information environment to provide them with near real-time information by which they can make more informed decisions. The information environment is where humans and now machines, observe, orient, decide and act and is therefore the principal environment of decision making. The information environment is made up of three dimensions (for the purpose of this publication will be referred to as domains): physical, information, and cognitive (see Figure I-1). These three are interrelated and occur simultaneously.

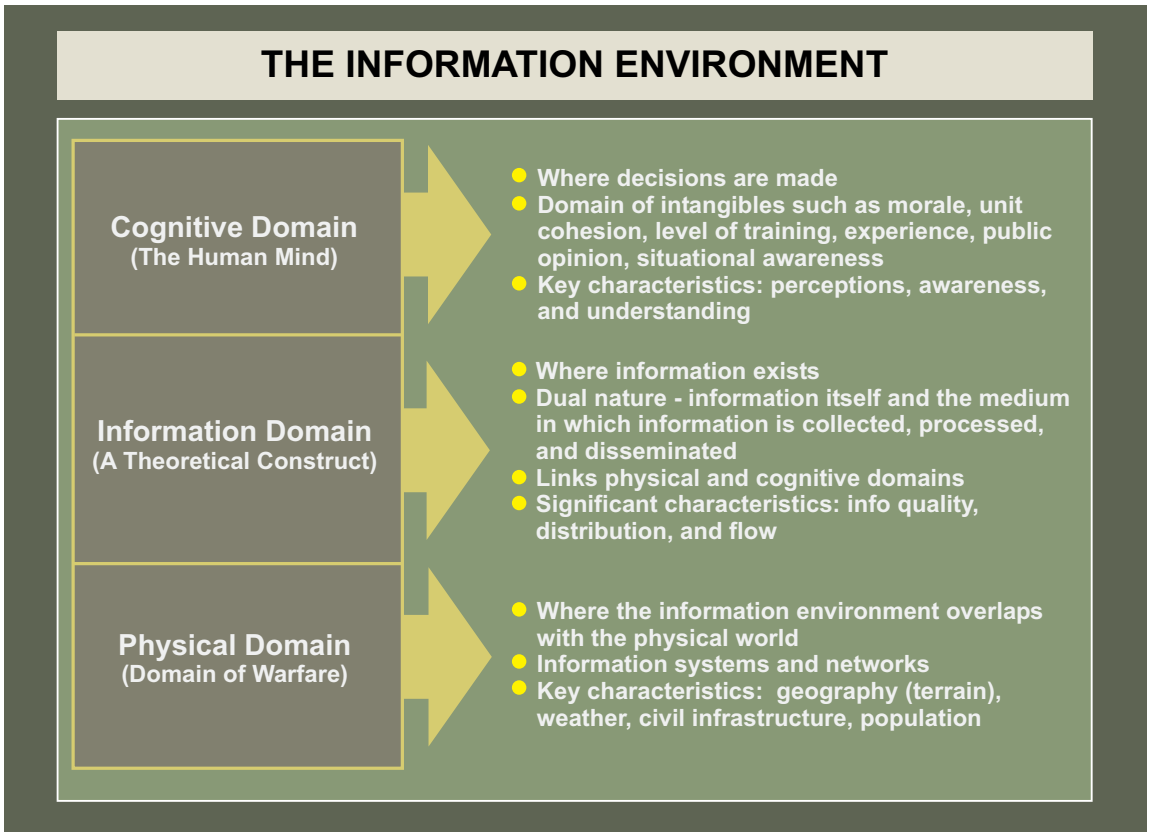


Figure I-1. The Information Environment

(1) **The Physical Domain.** The physical domain is composed of the physical computer and communications systems and supporting infrastructures that enable the military to plan, strike, protect, and maneuver and takes place across the ground, sea, air, and space environments. It is the traditional domain of warfare. It is also the domain 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 domain are the easiest to measure, and consequently, combat power has traditionally been measured primarily in this domain.

(2) **The Information Domain.** The information domain is the domain where information lives. It is the domain where information is created, processed, stored, manipulated, transmitted and shared among military decision makers and their forces. It is the domain where the command and control (C2) of modern military forces is communicated, and where commander's intent is conveyed. It consists of the substance of information . . . the 1's and 0's, written and spoken word, images, etc. Consequently, it is increasingly the information domain that must be protected and defended to enable a force to generate combat power in the face of offensive actions taken by an adversary. Thus, in the all-important battle for information superiority, the information domain is ground zero.

(3) **The Cognitive Domain.** The cognitive domain is the domain of the mind of the leader, warfighter, and the supporting populace. It is the most important of the three information domains, as decision makers must make decisions based upon information provided to them.

This domain is also affected by a commander's orders, training, tactics and other personal motivations. Many battles and wars are won or lost in the cognitive domain. Factors such as leadership, morale, unit cohesion, level of training and experience, situational awareness, and public opinion are elements of this domain.

~~b. Over the course of the last several decades, the geometric expansion of technical means used by individuals and groups to collect, process, or disseminate information is appreciated as a separate and distinct "environment" in which human activity takes place. In United States military terms, the separate "environments" of human activity are referred to as "dimensions." Joint Publication (JP) 3-0, *Doctrine for Joint Operations*, refers to the dimensions of land, sea, air, and space. Technological advances have been the catalyst driving the conceptualization of the information environment as another dimension of activity that military forces must learn to master. However, three fundamental aspects of the information dimension differentiate it from the other four dimensions.~~

~~(1) **The information dimension has human factor properties as well as physical and electronic properties.** All information resides in the mind, the physical world (has physical properties i.e. height, depth, length, etc.), or the electromagnetic spectrum. Individuals rely on their senses to perceive information in the physical world around them and use electronic equipment to send and receive information in the electromagnetic spectrum. Sensed information is "shaped" in the mind by a continuum of long and short-term factors. Longer-term factors may include genetics, culture, language, education, belief system, and experience. Shorter-term factors may include time, health, physical location, environment, and the number of competing "information streams" being received by the senses simultaneously. Beyond basic "survival" requirements, individuals use information for a variety of purposes including entertainment, education, and decision making. Individuals make decisions, consciously or subconsciously, from the mundane to profound, based on information "shaped" by the types of factors mentioned above.~~

~~(2) **All human activities take place in the information dimension; in addition to whatever physical dimension specific activities occur.** Because of the psychological property of the information dimension, wherever human activity occurs physically, such activity takes place simultaneously in the information dimension as well.~~

~~(3) **For the purpose of military doctrine, the information dimension, outside the mind, is entirely manmade.** The dimension's composition, both psychological and physical, consists of human thought and the infrastructure to gather, transport, store, process, and transform information to stimulate thought among individuals across space and/or time.~~

~~(4) **The concepts of location and movement within the information dimension are more complex than in the physical dimensions.** Location and movement of physical forms of information, or information infrastructure, is the same in the physical and information dimensions. However, electronic or mental forms of information may exist simultaneously in multiple physical locations may occur over multiple paths in multiple forms.~~

b. The development of computers and supporting information technology (IT) has given rise to the "Information Age." **One of the defining aspects of this age is the delegation of decision making to machines.** In previous eras, all decisions made were in the mind, whether individually or collectively. The history of the information age is a chronology of increasingly complex decisions made external to the mind by increasingly small and ubiquitous machines. Decisions made external to the mind are considered automated decisions throughout this publication.

c. **Technology has enabled information to be collected, processed, transported, and stored external to the human mind in quantities and at speeds that were incomprehensible only a few years ago.** While technology is making great quantities of information available to audiences worldwide, the types of perception-affecting factors mentioned above provide the context which individuals "use" to "translate" information sensed into knowledge. Knowledge, in turn, affects both subsequently received information and, when cumulatively considered (experience) with "judgment," becomes understanding.

d. **There are criteria of information that define its quality relative to its purpose.** Expressed a number of different ways in current literature, the criteria shown in Figure I-2 are from Joint Publication (JP) 6-0, *Doctrine for C4 Systems Support to Joint Operations*. Varying purposes of information require different applications of these criteria to define "valuable" information. There are both real and opportunity costs associated with obtaining quality information - that is, information well suited to its purpose. Costs such as those to acquire, process, store, transport, and distribute information are actual costs. Potential opportunities lost when expending time and resources (human, infrastructural, and fiscal) in the effort to acquire

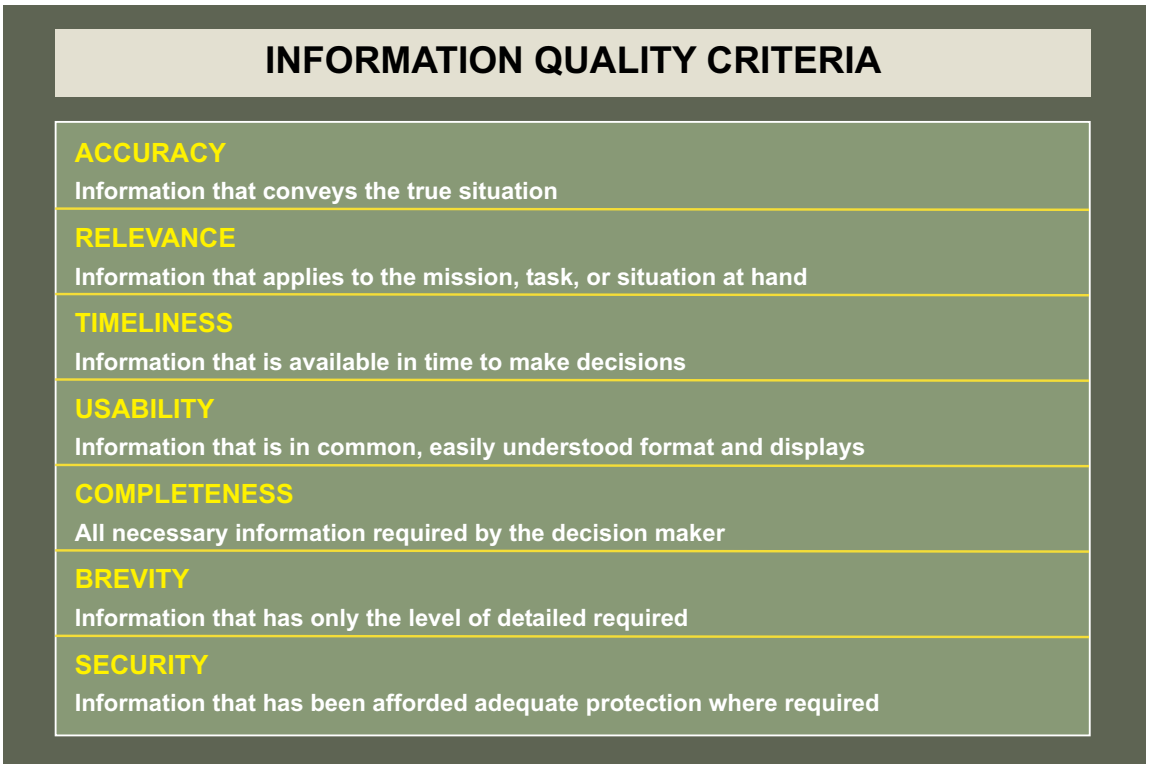


Figure I-2. Information Quality Criteria

quality information represent opportunity costs.

e. The fields of computer science, robotics, and artificial intelligence have given new appreciation to the complexity and agility of the human mind, which routinely makes decisions using all the information criteria in Figure I-2. Each decision relies on a different weighting of information criteria to make the "best" decision. As IT has progressed, increasingly complex decisions have proven well-suited for delegation to information systems. Other seemingly simple decisions are, even today, not well-suited for delegation to information systems. Decisions requiring primacy of timeliness, usability, and brevity of input quality were, early in the information age, discovered to be well-suited to information systems. Decisions requiring accuracy, relevance, and completeness of input continue to be more challenging without at least some human intervention in the decision-making process. The security of electronic decisions continues to be a race against the mind. Measures to secure information systems have proven often to be subject to newer means to defeat those measures.

f. **The finite amount of time and resources available to obtain quality information for any particular purpose or purposes is an important aspect in understanding the nature of human activity in the information dimension.** It is also fundamental to understanding the potential for IO to be a value-added concept in military operations. Whether decisions made are in the mind or electronically, the limited time and resources to "improve" quality of available information leave decision making subject to manipulation. In the context of planning and executing joint operations, decision making, and the information quality criteria related to decision making, are the most relevant to this doctrine. The criteria shown in Figure I-2 are discussed further, in relation to the potential various IO capabilities to affect specific criteria, in Chapters II, "Core, Supporting, and Related Information Operations Capabilities," and III, "Intelligence, Command, Control, Communications, and Computers Support to Information Operations." Chapter V, "Planning and Coordination," discusses how joint IO planning uses these quality criteria.

3. Military Operations and the Information ~~Dimension~~ Environment

a. **Information is an instrument of national power.** ~~As such, it has a diffuse and complex set of components with no single center of control.~~ Information ~~itself~~ is a strategic resource vital to national security. This reality extends to the US Armed Forces at all levels. Military operations, in particular, are dependent on many simultaneous and integrated activities that, in turn, depend on information and information systems.

b. **In modern military operations, commanders face a variety of information challenges.** Technical challenges include establishing and maintaining ~~command, control, communications, and computer (C4)~~ connectivity in ~~a~~ remote locations. ~~during a disaster relief or humanitarian assistance mission.~~ Operational challenges include the complexities of modern combat against a sophisticated adversary ~~who opposes friendly forces~~ with modern weapons and a sophisticated and growing IO capability. ~~information campaign.~~ Regardless of the size of their traditional military infrastructure, adversaries, including terrorist groups, can develop, purchase, or download from the Internet IO tools and techniques that enable them to attack the United States.

c. **Military forces operate in an information ~~dimension~~ environment, which changes over time.** 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 dimension for which military operations are planned and in which such operations are executed.

(1) Longer-term factors may include the various ways by which humans organize themselves (nation states, ~~groups,~~ tribes, families, etc.),~~;~~ group experience and interaction (i.e., anthropology, sociology, and history),~~;~~ regional influences (stability, alliances, economic relationships, etc.), and technological advances.

(2) Medium-term factors may include the rise and fall of organizational leaders, competition between organizations over resources or goals, development of specific technologies into information infrastructure, and the relative resources that various organizations can employ to take advantage of information technology and infrastructure.

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

d. The ubiquity of the information dimension in human activity combined with the speed and processing power of modern IT, both enhances and complicates military efforts to organize, train, equip, plan, and operate. ~~These complications and enhancements are discussed in later chapters. Traditionally, organization of military forces consists of units arranged in hierarchical chains of command. Historically, organization of specific units at each level of the chain of command matches their purpose and allows their leadership to direct unit activities within an appropriate span of control, consistent with purpose and available technology for command and control (C2). e.~~ Today, technology has opened the way to ~~attempt~~ ever-increasing span of control. ~~Military and civilian leaders anywhere can talk with individual squad leaders, ships captains or pilots on the other side of the world. However, span of control is practically determined by individual capability to absorb, process and react to available information on a prioritized basis consistent with competing demands, in a finite amount of time; rather than by available communication technology.f.~~ Militaries, as well as other human organizations, are challenged to adjust organizational size and function to balance almost unlimited global C2 ~~"~~reach~~"~~ with ~~still limited~~ finite human senses and the finite time available to the leadership at every level of command. These are challenges for adversaries as well as for the ~~United States~~ US and its ~~friends~~ allies.

~~g~~e. **United States forces perform their missions and prevail in an omnipresent, increasingly complex, information ~~dimension~~ environment**. To succeed, it is necessary for United States forces to gain and maintain "information superiority". In DOD ~~P~~policy, information superiority is ~~defined~~ described as the ~~capability to~~ 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. Finite time and resources dictate that information superiority be achieved and maintained temporarily,~~;~~ relative to a specific

adversary or adversaries, in support of a specific mission or missions, and within a specific timeframe.

(1) The forces possessing better information and using that information more effectively to gain understanding has a major advantage over its opponent. A commander that gains this advantage can use it to accomplish missions by affecting adversary perceptions, attitudes, decisions, and actions. However, information superiority is not static because, during operations, all sides continually attempt to secure its advantages and deny them to adversaries. The operational advantages of information superiority can take several forms, ranging from the ability to create a better operational picture and understand it in context, to the ability to shape the environment through the effective conduct of IO.

(2) Additionally, information superiority exists relative to an adversary. Recognizing this superiority can be difficult, but it exists when the information available to commanders allows them to accurately visualize the situation, anticipate events, and make appropriate, timely decisions more effectively than the adversary commanders can. In essence, information superiority enhances commanders' freedom of action and allows them to execute decisions and maintain the initiative. However, commanders recognize that without continuous IO designed to achieve and retain information superiority, adversaries may counter those advantages and possibly attain information superiority themselves. Commanders achieve information superiority by maintaining accurate situational understanding while creating a disparity between reality and how adversaries perceive it. The more IO shapes this disparity, the greater the friendly advantage.

f. **Adversaries.** It is becoming increasingly difficult to tell friend from foe in the Information Age. 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. To make matters more difficult, a military ally may also be an information adversary, such as a friendly country, which routinely practices economic/industrial espionage against their economic competitors. Potential adversarial IO attack techniques are numerous. Some, particularly electronic means, can be prevented by the simple application of cryptography, firewalls, and other network security techniques. Others are considerably more difficult to counter. Possible threat IO 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. The national intelligence community (IC) produces assessments of threat capabilities.

4. Fundamentals of Information Operations

a. ~~**The fundamentals of joint operations discussed in JP 3-0, *Doctrine for Joint Operations*, are applicable to IO.**~~ Like operations in the physical ~~dimensions~~ domains, IO involves military actions or the carrying out of strategic, operational, tactical, service, training, or administrative military missions in the information ~~dimension~~ environment. ~~.~~ As a military activity, IO are subject to the law of armed conflict (LOAC) and must comply with the principles of LOAC.

For a detailed discussion on LOAC, see JP 1-04, Joint Tactics, Techniques, and Procedures for Legal Support to Military Operations.

~~b. As a military activity in the information dimension, **IO is subject to the Laws of Armed Conflict (LOAC) and must comply with the principles of the LOAC including military necessity, proportionality, discrimination or distinction, and avoidance of unnecessary suffering of humanity**. A detailed discussion of the principles of LOAC can be found in Appendix S of JP 1-04, "Joint Tactics, Techniques and Procedures for Legal Support to Military Operations."~~

~~c~~b. Like other operations, **IO involves ~~movement, supply,~~ attack, defense, ~~and~~ maneuver, and supply needed to ~~gain~~ accomplish objectives across the range of military operations.** When IO requires attack and defense, attack consists of combinations of maneuver and fires~~, as in the physical dimensions~~. Defense in the information ~~dimension~~ environment is to counter~~s~~ an adversary's ~~maneuver and fires~~ action or perceived action in the information ~~dimension~~ environment. **Maneuver, fires, and support ~~are~~ can be accomplished physically, electronically, or psychologically in combination to support operations in both the physical ~~dimensions~~ domains and the information ~~dimension~~ environment.** ~~All aspects of joint operations require integration and synchronization across all dimensions of military activity.~~

(1) **~~Information~~ Maneuver.** **~~Information m~~Maneuver in the information environment is the deliberate positioning of information in military operations for presentation to target audiences (TAs).** As in the physical ~~dimensions~~ domains, specific IO tactics, techniques and procedures (TTP) may employ maneuver against adversaries in the information ~~dimension~~ environment or restrict an adversary's ability to maneuver in the information ~~dimension~~ environment.

(2) **~~Information~~ Fires.** Fires are used to produce ~~the~~ effects and can be the product of lethal or nonlethal weapons**.** Unlike conventional lethal weapons that destroy their targets through blast, penetration, and fragmentation, nonlethal weapons employ means other than gross physical destruction to achieve their intended effect. Nonlethal fires can be kinetic (such as ~~various crowd control weapons~~ leaflet drops) or nonkinetic (e.g., CNA, EA, etc.).

(a) **~~Information fires~~ Fires in the information environment can produce lethal, nonlethal, kinetic, or ~~are nonlethal and~~ nonkinetic effects.**~~,~~ ~~including~~ Such fires could include psychological, electromagnetic (EM), or cyber capabilities employed by military or terrorist organizations as force or threat of force as such organizations have historically employed force in the physical ~~dimensions~~ domains (land, sea, air, and space).~~.~~ The ~~concept of information~~ idea of fires in the information environment will require ~~provides the~~ legal ~~means~~ review to distinguish military activities in the information ~~dimension~~ environment that are subject to the rules of engagement (ROE) from those that are not. All ~~M~~military informational activities ~~that do not meet the criteria of information fires, such as information maneuver and intelligence,~~ require some level of legal review as they may be subject to ~~other moral, ethical,~~ policy or legal~~, or regulatory~~ constraints.

(b) ~~To qualify as information fires,~~ For an informational activity to be considered a form of fires in the **information** ~~dimension activity~~ environment it **must**: ~~1)~~ **involve the use or threat of use of** military **force**;~~,~~ ~~2)~~ **be employed by a nation, a nation's military**, ~~or~~ **a terrorist organization**s, other adversarial organizations, **(or** ~~their~~ **it's agent**s~~)~~;~~,~~ **and** ~~3)~~ **seek to achieve objectives traditionally pursued with force in international affairs (see Figure I-3).** ~~Whether~~ Qualification of such activity ~~qualifies~~ as a form of fires in the information ~~fires~~ environment is often situational dependent. ~~Information activity to employ equivalent capabilities for criminal purposes is not information fires but a matter of law enforcement.~~

(c) ~~Information fires~~ **Fires in the information environment may be employed with or without other information activities and/or conventional military force**, to achieve the traditional military objective of compelling an adversary to a specific course~~s~~ of action (COA). If applied in concert with conventional military force, ~~information~~ fires in the information environment may be in a supporting or a supported role ~~in specific military operations~~. ~~Information fires~~ Fires in the information environment are scalable from the strategic to the tactical levels of war. ~~Depending on the capabilities chosen and the TTPs employed, information fires~~ Fires in the information environment may be conducted covertly or overtly ~~by the originating unit or agent~~. ~~**Air, land, sea, space, and special operations forces have capabilities to deliver information fires. Likewise, all these forces must be protected from information fires.**~~ All forces that have capabilities to deliver fires in the information environment require protection within the information environment from similar fires.

(3) **Modern technologies enable** ~~information~~ **fires within the information environment to be employed without regard to international boundaries** from any geographic position where the appropriate information infrastructure exists. ~~For instance, information fires employed against the United States may be originated by adversary agents from within the borders of the United States or any of its allies and coalition partners. Who is responsible for countering such "internal" information fires is a matter of domestic and international law.~~

5. Principles of Information Operations

a. Success in military operations depends on acquiring and integrating essential information and denying it to the adversary. ~~As discussed in Chapter 1 section 3, **IO is new in name only**.~~ IO ~~represent merely United States "state-of-the-art" conceptualization,~~ encompass organization, planning for, and employment of, current capabilities to deliberately affect or defend the information ~~dimension~~ environment in ways that contribute to the achievement of combatant commander objectives. ~~b. The operational principles discussed in JP 3-0, *Doctrine for Planning Joint Operations*, apply to IO as well. IO plans and~~ employ~~s~~ military capabilities according to operational principles in the information ~~dimension~~ environment and defense against adversary information activities in support of military objectives.

NOMINAL DETERMINATION OF INFORMATION FIRES IN THE INFORMATION ENVIRONMENT

Information Environment Activity	Involves use or threat of force?	Who does it?	Objective?	Fires?
Electronic Attack (EA)	YES	Individuals, governments, militaries	Situational	Situational
Electronic Protection (EP)	NO	Individuals, businesses, governments, militaries	Protect electronics and use of electromagnetic spectrum	NO
Electronic Warfare Support (ES)	NO	Militaries	Intelligence gathering	NO
Computer Network Attack (CNA)	YES	Individuals, governments, militaries	Situational	Situational
Computer Network Defense (CND)	NO	Individuals, businesses, governments, militaries	Defense of computer networks	NO
Psychological Operations (PSYOP)	Situational	Militaries, governments, business	Influence	Situational
Deception	Situational	Individuals, businesses, governments, militaries	Mislead	Situational (Deception could involve electronic, psychological, or computer capabilities)
Various Security Measures	NO	Individuals, businesses, governments, militaries	Secure information and information infrastructure	NO
Intelligence Activities	NO	Individuals, businesses, governments, militaries	Obtain information	NO
Information Assurance (IA)	NO	Businesses, governments, militaries	Situational	NO
Public Affairs (PA)	NO	Individuals, businesses, governments, militaries	Inform	NO
Public Diplomacy (PD)	NO	Governments	Inform	NO

Figure I-3. Nominal Determination of ~~Information~~ Fires in the Information Environment

(1) **Core capabilities** are used exclusively to conduct and defend against military activities in the information ~~dimension~~ environment.

(2) **Supporting capabilities** may be used selectively in IO, but are also employed in other aspects of military activity.

(3) **Related IO capabilities** are constrained by United States moral, ethical and legal considerations from being considered part of information fire or other military activities, which affect the information ~~dimension~~ environment, but have a supporting role to play.

~~c~~b. **IO ~~is~~ are primarily concerned with affecting adversary ~~decisions~~ perceptions, actions, and decision-making processes, while at the same time ~~and~~ defending friendly decision-making processes, whether human or automated**. To accomplish this goal, joint IO efforts seek to affect the information ~~dimension~~ environment in which adversaries make decisions, and protect the friendly information ~~dimension~~ environment from adversary effects. IO includes three integrated functions of overriding importance.

(1) ~~Deter, discourage, dissuade, and direct~~ Influence, disrupt, corrupt, and usurp an adversary, thereby disrupting their unity of command and purpose while preserving our own.

(2) ~~Protect our plans and misdirect the adversary~~'s, Misdirect adversary's plans while protecting our own, thereby allowing friendly forces to mass effects to maximum advantage while the adversary expends their resources to little effect.

(3) Control ~~adversarial~~ adversary communications and networks and protect those of friendly forces, thereby crippling the ~~enemy's~~ adversary's ability to direct ~~an organized defense~~ organized operations while preserving effective C2 of friendly forces.

~~d~~c. **IO's ability to affect and defend decision~~s~~ making is based on five fundamental assumptions~~:~~.**

(1) Generally ~~T~~the quality ~~criteria~~ of information~~, relative to a specific purpose or purposes, are universal across geographic, linguistic, cultural, temporal, and organizational boundaries in imbuing specific types of information with value to decision makers, both human and automated.~~ that is considered valuable to human and automated decision makers is universal. However, the relative importance of each quality criteria of information may vary based on geographic, linguistic, cultural, religious, organizational, or personality influences.

(2) Predictable ~~D~~decisions are made ~~rationally~~ based on the information available ~~to decision makers~~ at the time influenced by cultural and personality factors.

(3) It is possible, with finite resources, to understand enough of the relevant aspects of the information ~~dimension~~ environment in which specific decision makers act and the processes they use to make decisions.

(4) It is possible to affect the information ~~dimension, psychologically, electronically, or physically,~~ environment in which specific decision makers~~, or groups of decision makers,~~ act ~~to advance military goals~~ through psychological, electronic, or physical means.

(5) It is possible to measure ~~T~~the effectiveness of ~~specific~~ IO actions ~~are measurable~~ in a timely manner in relation to their purpose.

~~e~~d. Since ~~all~~ most human activity takes place in the information ~~dimension,~~ environment ~~all human activity~~ it is potentially subject to IO. However, ~~**economy of force dictates that**~~ **only mission-related critical psychological, electronic, and physical points in the information ~~dimension~~ environment should be targeted, directly or indirectly, by IO**. The planning methodologies used to identify and prioritize such points ~~and the relative usefulness these methodologies~~ in planning IO ~~is~~ are discussed in Chapter V, "Planning and Coordination."

~~f~~e. **IO ~~are scalable~~ can produce effects and achieve objectives from ~~the national level, through~~ the strategic ~~and operational levels,~~ to the tactical level**. The ~~omnipresent,~~ real-time nature of the modern information ~~dimension~~ environment complicates the ~~determination~~ identification of the boundaries between these levels. In ~~this dimension~~ the information environment, tactical actions can have consequences up to the ~~national~~ strategic level and vice versa. Therefore, **all levels of Department of Defense (DOD) informational activities, including IO~~, at all levels,~~ should reflect and be consistent with broader national security policy and ~~strategy~~ strategic objectives**. ~~This aspect of the information dimension is discussed further in later chapters.~~

~~g. The quality criteria of information discussed earlier in this chapter, allow detailed analysis of the information dimension and military capabilities from both a friendly and adversarial perspective to evaluate opportunities and vulnerabilities that may be exploited in IO. Information systems, procedures, and IO capabilities to be cross compared and analyzed using the "lowest common denominator" of the quality criteria. Such an approach facilitates the efficient allocation of resources both in planning and in research and TTP development.~~

~~h~~f. **IO are full-~~time~~spectrum operations requiring extensive preparations ~~in peacetime~~.** ~~W~~well before crises develop~~.~~, Therefore, the IO ~~battlespace~~ environment should be prepared through activities such as intelligence, surveillance, and reconnaissance and extensive planning ~~activities~~.

~~i. Because IO is concerned with both affecting adversary decisions and defending friendly decisions, reference to "offensive" IO and "defensive" IO is convenient for discussion and planning purposes. In practice, the IO effort must be continuous and complementary across the offense/defense "spectrum" of possible, desirable, and feasible **actions**. In the paragraphs that follow, discussion of defense is abbreviated but no less important. **Offense and defense are different perspectives of the same effort**.~~

~~j~~g. **The ultimate strategic objective of ~~offensive~~ IO offensively is to affect adversary or potential adversary decision makers to the degree that will cause them to modify ~~personal~~ actions, or direct their subordinates to modify or cease actions, that threaten ~~United States~~ US national security interests**. The requirement to mutually support~~,~~ and ~~seamlessly~~ coordinate IO efforts across all theaters and levels of command is further complicated by the need to properly sequence IO actions at all levels of war to achieve cumulative and perhaps, multi-mission support of national security objectives. Additionally, ~~offensive~~ IO actions

executed through civilian controlled portions of the Global Information Grid (GIG), or which may cause unintended reactions of ~~United States~~ US or foreign populaces, must account for ~~moral, ethical,~~ US policy and legal issues, as well as potentially disruptive infrastructure issues, through civil-military coordination at all levels.

~~(1) Offensive IO seeks to achieve objectives at the various levels of command through discrete actions to modify the quality criteria of information present during military operations. These planned modifications shape the information dimension in ways that are advantageous to friendly forces.~~

(1~~2~~) **~~Offensive~~ IO may "target" human or automated decision making with specific actions**. Technology allows automated decision making to be targeted with increasing precision and affords more sophisticated ways to protect automated decision making. However, **targeting automated decision making, at any level, is only as effective as the human adversary's reliance on such decisions**. Targeting human decision making~~,~~ is problematical because of the ~~multiplicity of factors~~ complexity of the relationship between factors from a broad spectrum of sources that affect those decisions.~~, is more of an art than an exact science.~~ This complexity, which may appear to be overwhelming initially, affords planners multiple opportunities to apply a variety of TTPs. Effective implementation of the correct TTPs can result in disproportionately advantageous outcomes for friendly forces.

(2~~3~~) The focus of ~~offensive~~ IO offensively is on directly affecting the decision maker and the information ~~and data~~ in order to affect~~, indirectly,~~ the human decision maker's knowledge and understanding of the military situation. **IO can affect ~~data and~~ information in two basic ways**:

(a) By taking specific psychological, electronic, or physical actions ~~to~~ that add, modify, or remove information ~~itself~~ 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.

~~k~~h. Defensively, the ultimate objective at any level of IO is to prevent adversaries from affecting friendly leaders's decisions~~ with IO-like actions~~. ~~Because of the real-time, interconnected nature of the GIG,~~ **~~defensive~~ IO must account for an adversary's potential physical, electronic, and psychological reach.** ~~If adversary intelligence determines friendly vulnerabilities, and the adversary decides that specific, IO-like actions are useful to furthering their objective(s), electronic and psychological options potentially extend adversary reach worldwide.~~ There are three ~~principle~~ principal reasons ~~that~~ why IO~~-like actions~~ appeal to ~~United States~~ US adversaries today:

(1) **Vulnerability** - Such actions target well-known ~~United States~~ US commercial, civil, governmental, and military dependence on ~~modern~~ information infrastructure, as well as exploiting the open nature of democratic institutions.

(2) **Feasibility** - ~~United States~~ US technological and conventional military superiority make such options ~~feasible~~ more desirable for "asymmetrical" attacks.

(3) **Accessibility** – Seamless GIG and global media saturation give adversaries electronic and psychological access to ~~United States decision makers~~ the US population when physical access is denied.

~~**6. Framework of DOD IO Concept**~~

~~Core capabilities and their potential contribution to IO is discussed in further detail in Chapter II, *Core Information Operations Capabilities*. Supporting and related capabilities and their potential contribution to IO is discussed in Chapter III, *Information Operations Supporting and Related Capabilities*. Intelligence support is discussed in Chapter IV, *Intelligence Support to Information Operations*.~~

6. Information Operations' Relationship to Strategic Communication

a. In order to ensure consistent policy, themes and messages, the USG supported by DOD should develop and sustain an information strategy. This strategy guides and directs strategic communication activities across the information environment. Although strategic communication has not been defined by the USG, it can be described as the proactive and continuous process that responds to national security threats by identifying information threats and opportunities. It is the transmission of integrated and coordinated USG themes and messages that advance US interests and policies through a synchronized interagency effort supported by public diplomacy, public affairs, and related elements of IO, in concert with other political, economic, information, and military actions.

b. DOD public affairs, defense support to public diplomacy, and IO are distinct functions within DOD that have defined missions and should not be confused with strategic communication. Each function supports the wider concept of USG strategic communication but close coordination is essential to effective support to strategic communication.

7. Importance of Information Operations in Military Operations

a. History indicates that the speed and accuracy of information available to military commanders has a significant role in determining the outcome on the battlefield. Due to the information age, US military commanders rely on computer and communication systems. IO enables the accuracy of information required by US military commanders by defending our systems from exploitation by our 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 as asymmetric-based warfare that can be used to thwart US military objectives that are heavily reliant on information-based systems. This requires the US military to deploy defensive technologies and utilize leading-edge tactics and procedures to prevent our systems from being successfully attacked and penetrated.

1
2

Intentionally Blank

CHAPTER II
CORE, SUPPORTING, AND RELATED INFORMATION OPERATIONS CAPABILITIES

NOTE: The following replaces Chapters II and III from the First Draft.

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

Charles Ardant du Picq 1821 - 1870

1. Introduction

IO employs five core capabilities to achieve desired combatant commander effects or to prevent the adversary from achieving his desired effects: PSYOP, MILDEC, OPSEC, EW and CNO. These capabilities are operational in a direct and immediate sense; they either achieve critical operational effects or prevent the adversary from doing so. They are supported by five other capabilities: counterintelligence (CI), combat camera (COMCAM), physical attack, physical security, and information assurance (IA), and three related capabilities: defense support to public diplomacy (DSPD), public affairs (PA), and civil-military operations (CMO). Together these capabilities offer the commander a potent ability to affect and influence a situation. However, the potential for conflict between so many inter-related capabilities requires that their individual effects be coordinated, integrated and synchronized. The product of this coordination and integration is full spectrum IO.

2. Core Information Operations Capabilities

a. Of the five "core" capabilities for IO, 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 provide the JFC with his principal means of influencing his adversary and other target audiences and of assuring his own freedom of operation in the information environment. While not everything done within the core capabilities is directly IO, everything done will directly or indirectly have a bearing upon the achievement of IO objectives.

b. **Psychological Operations.** PSYOP are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce attitudes and behavior favorable to the originator's objectives. PSYOP are a vital part of the broad range of United States activities to influence foreign audiences and are the only DOD operations authorized to influence foreign TA directly through the use of radio, print, and other media. They complement but are not directly linked to the indirect provision of information through the civilian media by commanders and their PA staff. PSYOP personnel advise the supported commander on methods to capitalize on the psychological impacts of every aspect of force employment, as well as developing and planning delivery of specific PSYOP products, to achieve the overall campaign objectives. Unless otherwise directed by the Secretary of Defense, the Commander, United States Special Operations Command

(CDRUSSOCOM) exercises combatant command (command authority) (COCOM) over all assigned military PSYOP forces. When directed by the Secretary of Defense, CDRUSSOCOM transfers PSYOP forces to geographic combatant commanders. During a crisis, one of the first elements deployed to a supported commander is the PSYOP assessment team (POAT). The POAT provides staff support to the operations directorate (J-3) of the joint force. If the POAT assesses that significant PSYOP forces are required to support the JFC objectives, the POAT recommends to the JFC that a joint PSYOP task force (JPOTF) or PSYOP support element be established. The senior PSYOP officer in the operational area, normally the JPOTF commander, also may serve as the de facto joint force PSYOP officer. If the situation can be handled by augmenting the JFC's staff, the joint force PSYOP officer will ensure that component staffs are aware of the PSYOP products available. Working through the various component operations staffs, the joint force PSYOP officer will ensure continuity of psychological objectives, and themes to stress and avoid.

(1) **PSYOP as an IO Core Capability.** As one of the oldest and most established IO capabilities, PSYOP has a central role in the achievement of IO at the operational and tactical levels in support of the JFC. The development of the information environment to the point at which no piece of information can stand alone has meant that even tactical PSYOP activities can have strategic effects. The PSYOP staff must have a clear understanding of the government's themes and messages. The interrelated nature of PSYOP at all levels and across all IO capabilities demands a process of vetting to ensure that messages are complementary, appropriate and likely to be effective. This process is called Product Approval and a clear understanding of its importance and need for timely decisions is fundamental to effective PSYOP and IO. This is particularly the case in the early stages of operations given the time taken to develop and deliver a PSYOP product and for that product to have an effect on the target audience. PSYOP may be of particular value to the JFC in peacetime and pre/post-combat operations when other means of influence are not authorized. As a campaign develops, the Joint Prioritized Target List is the key methodology to integrate and deconflict PSYOP with physical attack and other types of non-kinetic fires. PSYOP convey information not only to intended PSYOP foreign TAs but also to foreign intelligence services and their customers. PSYOP messages must be coordinated with CI, MILDEC, and OPSEC to ensure secrecy, that CI operations are not compromised, and that messages reinforce the desired outcomes of CI and MILDEC as well as of PSYOP. There must be close cooperation and coordination between IO, PSYOP, and PA staffs in order to maintain credibility with their respective audiences. As the information environment develops, the opportunities for the delivery of PSYOP messages are expanding from the traditional print and radio to more sophisticated use of the Internet, fax messaging, text messaging and other emerging media. This will require further cooperation and/or coordination between EW, CNO, PA, CMO, and targeting staffs.

(2) **PSYOP Policy and Doctrine.** Policy includes Department of Defense Directive (DODD) S-3321.1, *Overt Peacetime Psychological Operations Conducted by the Military Services in Contingencies Short of Declared War*, and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3110.05 Series, *Joint Psychological Operations Supplement to the Joint Strategic Capabilities Plan FY 2004*. Joint doctrine is contained in JP 3-53, *Joint Doctrine for Psychological Operations*.

c. **Military Deception.** MILDEC is described as being those 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. MILDEC and OPSEC are complementary activities, the one seeking to encourage incorrect analysis in order to cause the adversary to arrive at specific false deductions while the other seeks to deny real information to an adversary in order to prevent him correctly deducing friendly plans. In order to be effective, MILDEC must be credible (at least a realistic friendly forces COA), verifiable (by the adversary's available and effective means of gathering information) and executable (by friendly forces). There is always a conflict between the resources required for deception and the resources required for the real operation and for this reason the deception plan should be developed concurrently with the real plan in order to ensure proper resourcing of both plans. 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 as 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 J-3 staff.

(1) **MILDEC as an IO Core Capability.** MILDEC is fundamental to successful IO. It exploits the adversary's own information systems, processes and capability to develop vulnerability. MILDEC relies upon the adversary's information gathering capabilities being fed a consistent message across the full range of his effective sensors. 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 have a part to play in the development of successful MILDEC and in maintaining its credibility over time. PA should not be involved in the provision of false information, but must be aware of the intent and purpose of the deception plan in order not to inadvertently compromise it.

(2) **MILDEC Policy and Doctrine.** Joint policy is contained in CJCSI 3211.01C, *Joint Policy for Military Deception*. For more detailed discussion see JP 3-58, *Joint Doctrine for Military Deception*.

d. **Operations Security.** 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.

(1) **OPSEC as an IO Core Capability.** OPSEC denies the adversary the information that he needs in order to correctly assess friendly capabilities and intentions. It is both a tool of

IO in itself, hampering the adversary's use of his own information systems and processes, and a necessary support to all friendly IO capabilities. In particular, OPSEC complements MILDEC, denying an adversary the information he requires 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 that might be easily countered are not compromised. The process of identifying essential elements of friendly information (EEFI) 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 OPSEC must be complemented by other types of security including physical security, security measures and programs in IA, computer network defense (CND), and personnel programs that screen personnel and limit authorized access.

(2) **OPSEC Policy and Doctrine.** Policy is contained in DODD 5205.2, 29 Nov 1999, *DOD Operations Security Program*, and CJCSI 3213.01 Series, *Joint Operations Security*. JP 3-54, *Joint Doctrine for Operation Security*, provides more detailed discussion.

e. **Electronic Warfare.** EW refers to any military action involving the use of EM and directed energy to control the EM spectrum or to attack the adversary. EW includes three major subdivisions: EA, electronic protect (EP), and electronic warfare support (ES). EA is the subdivision of EW involving 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 is the subdivision of EW 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 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.

(1) **EW as an IO Core Capability.** EW is the IO capability available to gain and maintain dominance of the EM spectrum during joint operations. EW contributes to the success of IO by using maneuver, attack, and defense 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 use 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 EW is involved in all aspects of IO. All of the core, supporting, and related IO capabilities either directly use EW to contribute to the development of their own effects, e.g. PSYOP, OPSEC, CNO, and MILDEC, or indirectly benefit from EW, e.g. IA, CI, CMO, and PA. In order to deconflict EW, and more broadly all military usage of the EM spectrum, all joint operations require a joint restricted frequency list (JRFL). This list specifies protected

frequencies that should not be disrupted either because of friendly use or friendly exploitation. This is maintained and promulgated by command, control, communications, and computer systems directorate of a joint staff (J-6) in coordination with J-3 and the Joint Commander's Electronic Warfare Staff (or an Electronic Warfare Coordination Cell (EWCC), if delegated). JP 3-51 *Joint Doctrine for Electronic Warfare*, discusses the specifics of JRFL development.

(2) **EW Policy and Doctrine.** Policy includes DODD 3222.4, 31 Jul 1992, *DOD Electronic Warfare and Command and Control Warfare Countermeasures*, and CJCSI 3210.03 Series, *Joint EW Policy*. JP 3-51, *Joint Doctrine for Electronic Warfare*, provides a more detailed discussion.

f. **Computer Network Operations.** CNO is one of the latest capabilities to be developed in support of military operations and stems from the very wide use being made of computers, and in particular networked computers, by both developed and developing militaries and other adversaries. CNO, along with EW, is used to attack, 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, or degrade information resident in computers and computer networks, or the computers and networks themselves. CND are 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. These 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 are enabling operations and intelligence collection conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

(1) **CNO as an IO Core Capability.** The increasing reliance of even unsophisticated militaries and terrorist groups on computers and computer networks for the passage of information, operational functions, and the C2 of forces means that all three aspects of CNO have a part to play in IO and may support or be supported by any of the core, supporting or related capabilities of IO. As the capability of computers and the range of their employment broadens so new vulnerabilities and opportunities will continue to develop. As with EW, 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. All aspects of CNO may also support, and be reliant upon, the space control mission area. Specific space control capabilities may conduct or contribute to CNO; these should be integrated and synchronized as part of the overall IO and will, for instance, require deconfliction within the JRFL. The doctrinal use of CNO capabilities in support of IO is discussed further in Appendix A, "Supplemental Guidance," to this publication.

(2) **CNO Policy and Doctrine.** Policy guidance is found in DODD O-8530.1, *Computer Network Defense (CND)*, and DOD Instruction (DODI) O-8530.2, *Support to Computer Network Defense (CND)*. Appendix A, "Supplemental Guidance," to this publication provides further discussion.

g. **Mutual Support Between IO Capabilities.** Figure II-1 provides a simplistic depiction of how the core IO capabilities are linked together and therefore interdependent. This also holds true for the relationship of the individual core, supporting, and related capabilities with one another. 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 inter-relationships 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 full spectrum IO across the range of military operations depends upon a full understanding of this inter-relationship between capabilities. Only then can they be properly and effectively integrated through the processes discussed in Chapter V "Planning and Coordination."

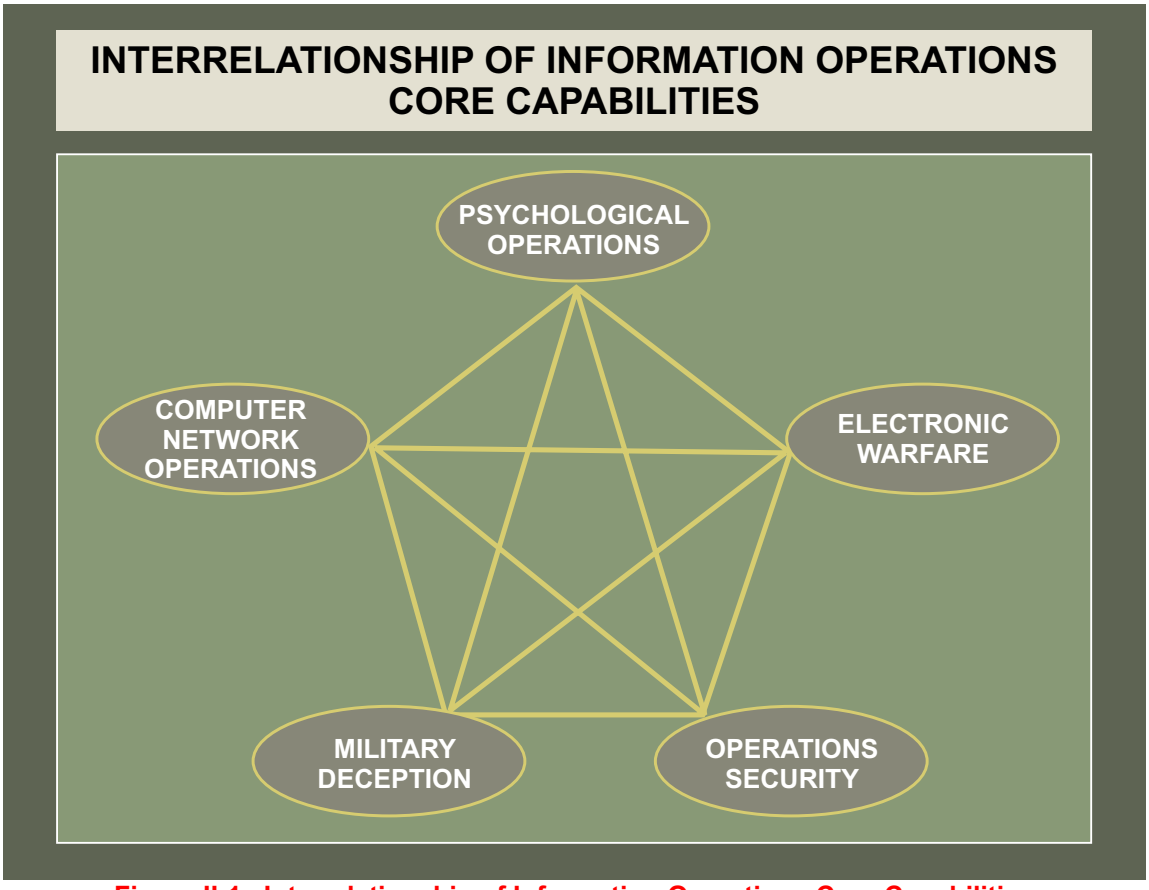


Figure II-1. Interrelationship of Information Operations Core Capabilities

3. Information Operations Supporting Capabilities

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

b. **Information Assurance.** IA is defined as measures that protect and defend electronic information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes protection, detection, response, restoration, and reaction capabilities and processes to shield and preserve information and information systems. IA is necessary to gain and maintain information superiority. IA requires a defense-in-depth 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 outside DOD controlled networks. In joint organizations, IA is a responsibility of the J-6.

c. **IA as a Supporting Capability for IO.** IO depends on IA to protect its information and to assure continuous capability. IA and IO have an operational relationship in which IO is concerned with the coordination of military activities in the information environment while IA protects the electronic and automated portions of the information environment. IO is reliant on IA to protect such infrastructure so that it is available to position information for influence purposes and for the delivery of some types of information to the adversary. In particular IA and all aspects of CNO are inter-related and rely upon each other to be effective. Likewise, IA is reliant 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.

d. **IA Policy and Doctrine.** For detailed policy guidance see DODI O-8500.1, *Information Assurance*, DODI O-8500.2, *Information Assurance Implementation*. Joint policy is established in CJCSI 3401.03, *Information Assurance Readiness Metrics*, and CJCSI 6510.01 Series, *Information Assurance and Computer Network Defense*.

e. **Physical Security.** Physical security is that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. 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.

(1) **Physical Security as a Supporting Capability for IO.** Like IA, physical security serves many functions in addition to the protection of information and information systems. Just as IA protects friendly electronic information and information systems, physical security protects physical facilities containing information and information systems worldwide. Physical security will often contribute 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/plans directorate of a joint staff as early as possible in the planning process. IO actions that rely on physical access to adversary information or information systems in rear areas must account for adversary physical security measures.

(2) **Physical Security Policy and Doctrine.** Physical security is discussed in JP 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, and in general in JP 3-10, *Joint Doctrine for Rear Area Operations*. Appendix F of JP 3-10.1, *JTTP for Base Defense*, contains a more detailed discussion.

f. **Physical Attack.** The concept of attack is fundamental to military operations. Attack consists of combinations of operational elements including fires, maneuver, and support. The phrase "physical attack" differentiates the use of kinetic fires (to include kinetic, nonlethal fires) from non-kinetic fires. Kinetic weapons may be employed against physical targets, including physical information targets. Both kinetic and non-kinetic fires are integrated and synchronized in joint operations through the targeting process.

(1) **Physical Attack as a Supporting Capability for IO.** Physical attack can be employed in support of IO as a means of influencing target audiences and IO capabilities, particularly but not exclusively PSYOP, can be employed in support of physical attack in order to maximize the effect of that attack on the morale of an adversary. The integration and synchronization of kinetic weapons with IO and vice versa 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, IO planners must be able to define the effects they seek to achieve and targeting staffs must have sufficient knowledge of IO capabilities to incorporate them into targeting products. In particular, the fast pace of air operations makes the coordination of the IO effort with the process to develop and update operational planning and execution products (e.g., the air tasking order) a critical part of planning and executing IO. Considerations of targeting are discussed in more detail in Chapter V, "Planning and Coordination."

(2) **Policy and Doctrine for Physical Attack.** Physical attack is addressed in a variety of policies and doctrine publications including: JP 2-01.1, *Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting*, JP 3-01.4, *JTTP for Joint Suppression of Enemy Air Defenses (J-SEAD)*, JP 3-03, *Doctrine for Joint Interdiction Operations*, JP 3-05.2, *JTTP for Special Operations Targeting and Mission Planning*, JP 3-09, *Doctrine Joint Fire Support*, and JP 3-60, *Joint Doctrine for Targeting*.

g. **Counterintelligence.** 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 terrorists. The CI program on joint staffs is a responsibility of the counterintelligence and human intelligence staff element of the intelligence directorate.

(1) **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 and at the same time to identify opportunities for IO. CNO, to include CNE, provide the tools to conduct CI operations. For the IO planner, CI analysis offers a view of the adversary's information gathering efforts. From this, CI can develop the initial intelligence target opportunities that provide access to the adversary for MILDEC information, for PSYOP products, and for CNA/CNE actions.

(2) **CI Policy and Doctrine.** Policy is established in various directives and instructions including DODD 5240.2, *Counterintelligence (CI)*, DODI 5240.6, *Counterintelligence Awareness Briefing Program*, DODI 5240.4, *Reporting Counterintelligence and Criminal Violations*, DODI 5240.10, *DOD Counterintelligence Support to Unified and Specified Commands*. Doctrine is discussed in more detail in JP 2-01.2, *Joint Doctrine, Tactics, Techniques, and Procedures for CI Support to Operations*.

h. **Combat Camera.** The COMCAM mission is to provide the Office of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff (CJCS), the Military Departments, the combatant commands, and the joint task force (JTF) with a directed imagery capability in support of operational and planning requirements during wartime operations, worldwide crises, contingencies, and joint exercises. COMCAM is responsible for rapid development and dissemination of products that support strategic and operational IO objectives. The COMCAM program belongs to Defense Visual Information, which falls under the Assistant Secretary of Defense for Public Affairs. When deployed, operational control (OPCON) of COMCAM forces can be delegated to any echelon of command at the discretion of the JFC and subordinate commanders. COMCAM should be assigned to the IO function at the JFC, component, and subordinate unit levels for operational proponency, planning, synchronization, and direction necessary for mission accomplishment. Most large JTF or commander, joint task force organizations will have a Joint COMCAM Management Team assigned to manage COMCAM in that area of responsibility (AOR), 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.

(1) **Combat Camera as a Supporting Capability for IO.** COMCAM supports all of the capabilities of IO that use images of US or friendly forces in their execution, whether to influence an adversary or support US forces or allies. They provide images for PSYOP, MILDEC, PA, and CMO use, but can also be used for BDA/measure of effectiveness (MOE). COMCAM can also provide operational 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 capabilities, means that COMCAM imagery can be provided to the professional news organizations by PA when they are unable to produce their own imagery.

(2) **Combat Camera Policy and Doctrine.** For detailed policy guidance see DODD 5040.4 and CJCSI 3205.01A. Joint doctrine is contained in *Multi-Service Tactics, Techniques and Procedures for Joint Combat Camera (COMCAM MTTP)* of Mar 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 in the IO planning process. This will require 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 in order to provide direct and timely advice to IO staff.

b. **Public Affairs.** PA operations are defined as those public information, command information, and community relations activities directed toward both the external and internal publics with interest in DOD. PA is one of six major information functions essential for joint forces information superiority and credible PA operations are necessary to support the commander's mission and maintain essential public liaisons throughout the spectrum of conflict. PA's principal focus is to inform the American public and international audiences in support of combatant command public information needs at all levels (see Figure II-2). JFCs communicate information about joint operations to domestic and international audiences through PA.

(1) **PA as a Related Capability to IO.** 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, public affairs officer membership in the IO staff will enable PA activities to be integrated, coordinated, and deconflicted with IO. While audiences and intent differ, both PA and IO ultimately support the dissemination of information, themes, and messages adapted to audience. PA contributes to the achievement of military objectives, for instance, by countering adversary disinformation through the publication of true stories. 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 threats, for the media and the military. The PA staff has a key role to play in establishing ground rules for both the embeds and those with whom they are embedded. Many of the nation's adversaries' leaders rely on limiting their population's knowledge to remain in power. PA and other IO activities must be coordinated and synchronized to ensure consistent themes and messages are communicated to avoid credibility losses. However, inherent in effective coordination and collaboration with IO is the necessity for PA to maintain its institutional credibility. In addition, PA may have a valuable media monitoring capability that can contribute to IO MOE.

(2) **PA Policy and Doctrine**. DODD 5122.5 provides guidance for PA and JP 3-61, *Doctrine for Public Affairs in Joint Operations*, provides more detail about joint PA.

c. **Civil-Military Operations.** CMO are the activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace. 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

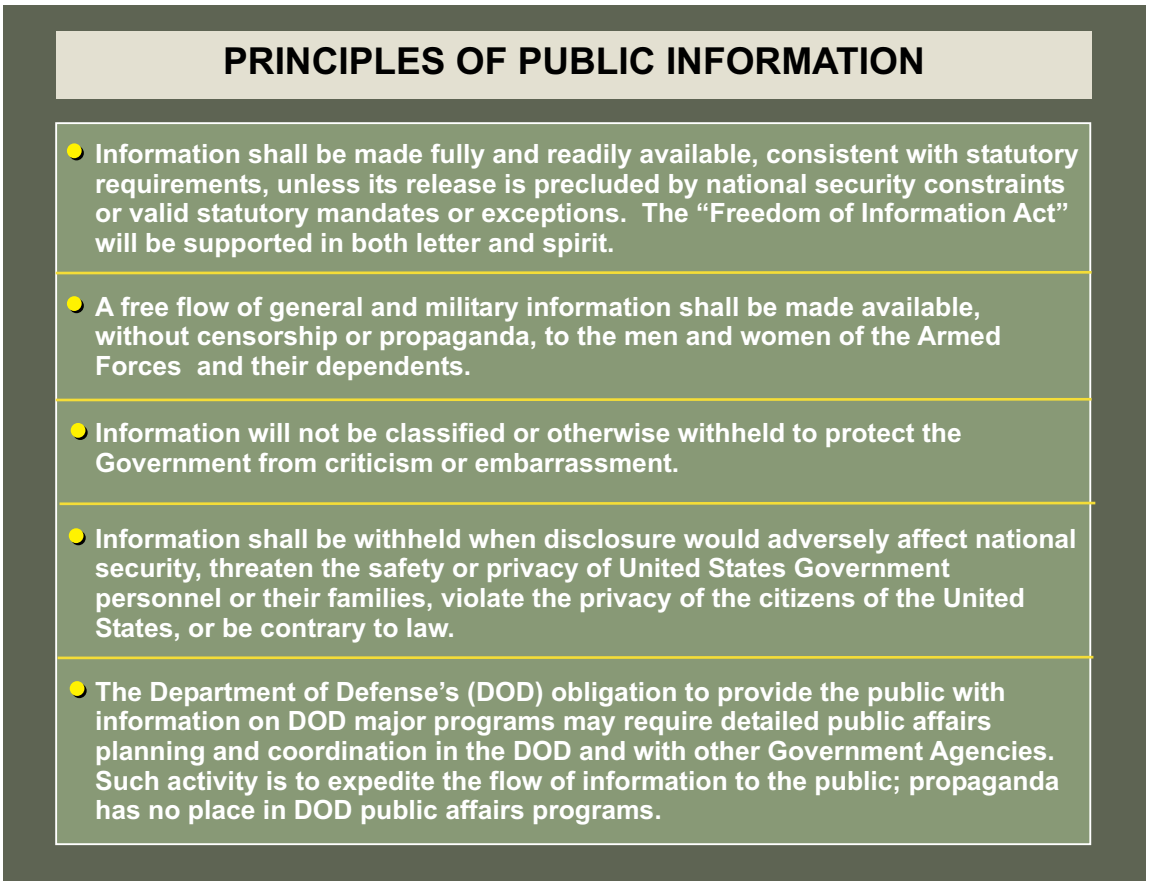


Figure II-2. Principles of Public Information

operations to support US national security objectives. CMO can occur in friendly, neutral, or hostile operational areas to facilitate military operations and achieve United States objectives. 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) units, by other military forces, or by a combination of CA and other forces. Certain types of organizations are particularly suited to this mission and will form the nucleus of CMO efforts. 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, act as enablers.

(1) **CMO as a Related Capability to IO.** Depending upon the nature of the mission and the phase of the operation, CMO may play a greater or lesser part in the overall conduct of IO and of military operations. Like PSYOP, CMO can be particularly effective in peacetime and pre/post-combat operations when other capabilities and actions may be constrained by ROE. Early consideration of the civil-military environment in which operations will take place will be important. As with PA, the CMO staff also has an important role to play in the development of wider IO plans and objectives. As the accessibility of information to the widest public audiences increases and as military operations cease to be conducted in a closed environment so the importance of CMO to the achievement of operational objectives, and particularly IO objectives will increase. At the same time the direct involvement in CMO of 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.

(2) **CMO Doctrine.** CMO is discussed in detail in JP 3-57, *Joint Doctrine for Civil-Military Operations*.

d. **Defense Support to Public Diplomacy and Strategic Communication.** DSPD is those activities and measures taken by DOD components, not solely in the area of IO, to support and facilitate overt public diplomacy efforts of the USG and its departments and agencies. It ensures that DOD sends a coherent and compelling message in concert with other USG agencies and in support of the Department of State who maintain the lead for Public Diplomacy (PD), with DOD in a supporting role. These strategic activities, and specifically the military's role in it, will be of increasing importance in the future, particularly in peacetime and pre/post-combat operations when ROE may not allow the use of other capabilities available to the USG and the JFC.

(1) **DSPD and IO.** DOD contributes to PD and the larger context of USG Strategic Communication by coordinating its overt information activities such as PA, IO and other military activities, including the deployment of forces and states of readiness and alert, with other agencies as part of an integrated and synchronized effort. This requires a high degree of coordination not only between departments but also within the DOD, between physical activities and those in the information environment. Much of the operational level IO activity conducted in any theater will be directly linked to PD objectives.

(2) **DSPD Policy.** DSPD is defined and DOD policy for DSPD is briefly outlined in [Formal Coordination Draft] of DODD 3600.1, *IO Policy*.

CHAPTER III
INTELLIGENCE, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS SUPPORT TO INFORMATION OPERATIONS

NOTE: The following replaces Chapters IV and V from the First Draft.

> *"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. General

Like all other aspects of joint operations, IO requires effective intelligence, command, control, communications, and computer (C4) support. IO is intelligence intensive in particular and therefore successful planning, employment, and assessment of IO demands detailed and timely intelligence. This chapter briefly discusses how intelligence and C4 support the planning and execution of IO.

2. Intelligence, Surveillance, and Reconnaissance Support to Information Operations

IO requires an understanding of the information environment because, 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 IO planners. This requires intelligence on relevant portions of the human factors, electronic, and physical aspects 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 adversary decision-making processes and determine the appropriate capabilities necessary to achieve operational objectives, commanders and their staffs must have current information on relevant physical, electronic, and human factor properties of the information environment and assessment of ongoing IO activities.

(1) **Physical Properties of the Information Environment.** Physical properties of the information environment require that IO include locations and capabilities of information infrastructure and adversary information capabilities. Physical properties may include:

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

(b) Organization of infrastructure and capabilities.

(c) Types and quantity of information infrastructure and capabilities (which specific makes, models, and how many).

(d) Power generation and distribution systems (if electronic forms of information are transmitted via power systems, such information and associated technical methods might be considered electronic properties).

(2) **Electronic Properties of the Information Environment.** Electronic properties of the information environment include those relevant to the electronic collection, transmission, processing, storage, and display of information by electronic means. Different electronic properties may be affected by different military capabilities such as EW and CNO. Electronic properties of the information environment include:

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

(b) Technical design of electronic information infrastructure.

(3) **Human Factor Properties of the Information Environment.** Human factor 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. Human factor properties may include:

(a) Cultural and societal factors affecting attitudes and perceptions such as language, education, history, religion, 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 of key decision makers.

(d) Psychological profile of key individuals and groups (both influential and decision makers).

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

(f) Laws, regulations, and procedures relevant to information and decision making, decision-making processes, capability employment doctrine, and TTP.

(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, electronic, and human factor 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 (electronic), the identity of owners and key personnel, and the credibility or popularity of each station (psychological).

b. **Intelligence Support to IO Targeting.** Intelligence support is an integral part of IO targeting. A sequential overview of intelligence support to IO targeting includes:

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

(2) Identify individual targets relevant to specified adversary decision making.

(3) Develop target set(s) for identified targets.

(4) Identify lethal and nonlethal effects appropriate to target set(s).

(5) Predict the expected consequences of identified effects.

(6) Coordinate with planning personnel to establish priority of intelligence effort during execution.

(7) Monitor friendly IO during execution phase (which may extend before and after execution of conventional operations).

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

(9) Evaluate the outcome of executed fires for lethal and nonlethal effects.

(10) Provide BDA for IO targets subject to the timeliness considerations.

3. Intelligence Considerations in Planning Information Operations

a. The dynamic and pervasive 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 include:

(1) **Intelligence Resources are Limited.** Information collection requirements are almost limitless. Commanders and their staffs must work with their intelligence directorate of a joint staff (J-2) personnel to identify and prioritize AOR requirements to the IC both at the theater and national level.

(2) **Collection Activities are Legally Constrained.** The seamless nature of the information environment complicates compliance with legal constraints so, when appropriate, the IC implements technical and procedural methods to ensure compliance with legal constraints. Additionally, intelligence must be supplemented with information provided by law enforcement or other sources, when necessary and legal, to plan IO.

(3) **IO Intelligence Often Requires Long Lead Times.** The intelligence necessary to affect adversary decisions often requires that specific sources and methods be positioned and employed over time to collect the necessary information and conduct analysis 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.

(4) **Information Environment is Dynamic.** The information environment changes over time according to different factors. Physical changes may occur more slowly than electronic or human factors changes, and may be easier to detect and analyze than human factors changes. Commanders and their staffs must understand both the timeliness of the intelligence they receive and the differing potentials for change of various aspects of the information environment.

(5) **Properties of the Information Environment Affect Intelligence.** Collection of physical and electronic information is objectively measurable by location, quantity, etc. While identification of key individuals and groups of interest may be a relatively straightforward challenge for the IC, the relative importance of various individuals and groups, their psychological profiles, and how they interact is not easily agreed upon nor quantified. Commanders and IO planners must have an appreciation for the subjective nature of intelligence on psychological profiles and human nature.

b. **Deconfliction of Planned IO with Intelligence.** Coordination should occur among intelligence targeting, IO, and collection processing personnel for deconfliction purposes. The requirement for thorough intelligence gain/loss and political/military assessments, when determining which targets to select for physical destruction, is central to the integrating effort of IO and cannot be overemphasized.

c. **Popular Perceptions.** The perceptions of foreign populations are an integral part of national interaction (political, economic, etc.) and policies towards the United States. Geographic combatant commanders require feedback concerning existing and changing foreign perceptions within their AORs on a continuing basis to support theater security cooperation planning, joint operation planning and execution system (JOPES) planning, and a wide variety of other activities. To help with this requirement, intelligence resources contribute to monitoring perceptions and attitudes of foreign populations and provide feedback to geographic combatant commanders.

d. **Priority of Effort.** The potential requirement to collect, analyze, and produce detailed intelligence of the granularity required for IO far exceeds the resources of the IC. Priority of effort in assigning intelligence resources to IO-specific tasking 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.

4. Sources of Intelligence Support

a. Through the 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 coalition partners.

b. 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.

5. Command, Control, Communications, and Computer Systems Support to Information Operations

a. Joint C4 systems support the warfighting commander across the range of military operations. DOD C4 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 C4 systems, which support other C4 requirements. Personnel responsible for IO or IO support at each DOD component use C4 systems available to other command personnel in compliance with appropriate IA, information management (IM), and administrative policies. The IO officer, or other designated person, provides C4 system support requirements through staff procedures established locally. Whether core capability staff sections submit their C4 support requirements through the IO officer is command specific. At each command, IO C4 requirements are prioritized with other unit or organizational C4 requirements. During operational planning, IO and capability-specific frequency and bandwidth requirements are negotiated as part of the JOPES or other designated planning process.

b. **Reference.** A further discussion of C4 systems support to joint operations can be found in JP 6-0, *Doctrine for C4 Systems Support to Joint Operations*, and other 6-series publications.

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. General

~~The need to gain and maintain information superiority to accomplish assigned missions, requires that the Department of Defense gain and maintain proficiency in all recognized information functions necessary to achieve that goal. As one of these necessary functions, IO is a necessary and integral part of joint operations. The Secretary of Defense delegates responsibilities for oversight of IO within the Office of Secretary of Defense (OSD) and designates responsibilities for specific aspects of IO or IO support as discussed in DODD 3600.1, IO Policy. The CJCS and the Joint Requirements Oversight Council (JROC) identify, assess and prioritize joint IO capabilities according to policy established in CJCSI 3170.01 Series, Joint Capabilities Integration and Development System. The Secretaries of the Military Departments train, equip and provide forces and capabilities to combatant commands through Service components as described in JP 0-2, Unified Action Armed Forces. Combatant commanders plan and execute IO as an integral part of joint operations.~~ This chapter describes ~~joint commander's~~ the JFC's authority for IO, specific responsibilities established in DODD 3600.1, *IO Policy*, and the *Unified Command Plan (UCP)*, command relationships between the DOD components responsible for IO, the organization of combatant command and JTF staffs for IO, and joint board, processes, and products related to IO.

2. Authorities and Responsibilities

a. **Authorities.** Authority to plan and execute IO as an integrated part of joint operations is inherent in ~~combatant command (command authority) (~~COCOM~~)~~. ~~The Unified Command Plan (UCP) divides exercise of authority among combatant commanders.~~ The electronic and human factor properties of the information ~~dimension~~ environment and available military capabilities to affect those properties, complicates the planning and execution of IO ~~exercise of COCOM~~. IO in one combatant command AOR may affect other ~~AOR's~~ AORs directly or indirectly. To address this complication, the President has given Commander, United States Strategic Command (~~COM~~CDRUSSTRATCOM) specific authority and responsibility to coordinate IO (core capabilities) across combatant command AOR ~~and functional~~ boundaries.

b. **Responsibilities.**

(1) Responsibilities for IO established in DODD 3600.1, *IO Policy*, include:

(Placeholder for responsibilities from approved revision of 3600.1)

(2) In accordance with change 2 to Unified Command Plan for Fiscal Year '02 ~~COM~~CDRUSSTRATCOM integrates and coordinates DOD IO that cross geographic AOR boundaries or core capability functional 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.

(d) ~~Identifying desired characteristics and capabilities for DOD-wide CND, planning for DOD-wide CND, and directing DOD-wide CND.~~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 ~~IO~~ Information Operations Organizational Roles and Responsibilities

a. **Joint Staff.** ~~The role of the Joint Staff is to assists the Chairman of the Joint Chiefs of Staff with responsibilities assigned by law, the President, Secretary of Defense, regulation, and tradition.~~ 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 ~~section~~ divisions of the Joint Staff J-3 provide~~s~~ IO specific advice and advocate~~s~~ Joint Staff and combatant commands IO interests and concerns ~~in Joint Staff administrative processes~~ within DOD and interacts with other organizations and individuals on behalf of the Chairman. CJCSI 3210.01 Series, *Joint Information Operations Policy ~~for IO~~*, provides specific policy guidance on IO responsibilities and functions of the Joint Staff.

b. **Combatant Commands.** CDRUSSTRATCOM's specific authority and responsibility to coordinate IO across 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 engagement goals incorporated in Theater Security Cooperation Plans (TSCP), shaping the operational environment for potential employment during periods of heightened tensions, or in support of military operations upon initiation of hostilities. It is entirely possible

that in a given theater, the combatant commander will be "supported" for select IO within theater 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 ~~centrally planned and decentrally executed~~ accomplished through centralized planning and decentralized execution. Joint-level planners should resist the temptation to plan in too great of detail to facilitate plan flexibility during execution and allow component staffs to develop plan details based on resource availability, constraints, and other factors. ~~JP 5-0, *Doctrine for Planning Joint Operations*, JP 5-00.1, *Joint Doctrine for Campaign Planning*, and JP 5-00.2, *Joint Task Force(JTF) Planning Guidance and Procedures*, provide details on joint planning.~~ The specifics of planning IO as an integral part of joint plans is discussed in detail Chapter V, "Planning and Coordination."

For more discussion on joint planning see JP 5-0, Doctrine for Planning Joint Operations*, and JP 5-00.2,* Joint Task Force Planning Guidance and Procedures.

c. **Functional and Service Components.** Functional components are normally responsible for detailed planning and execution of IO. Service components provide IO support ~~to JFC's and their functional components~~ as directed by ~~their chain of command~~ the JFC. IO planned and conducted by functional components must be conducted within the parameters established by national and joint force headquarters. At the same time, functional component commanders and their subordinates must be provided sufficient flexibility and authority to respond to local variances in the information environment. Component commanders determine how their staffs are organized for IO. Both Service and functional component commanders normally designate personnel to liaise between the JFC's headquarters and component headquarter staffs.

d. **Subordinate JFC.** Subordinate JFCs plan and execute IO as an integrated part of joint operations to carry out assigned missions within their AOR. 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 ~~IO~~Information Operations

The principal staffs that may be involved in IO planning are the **combatant command**, **subordinate joint force command(s)**, and **component staffs**. The circumstances in which these staffs conduct IO may affect the optimal organization.

a. **Combatant Command Organization. Combatant command staffs,** supported by the National Security Agency (NSA) and other Defense and intelligence 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 the JOPES to carry out planning responsibilities. ~~During crisis or other short notice operations, the JOPES process is entered at the phase dictated by circumstances.~~ The command which is designated the supported command will receive guidance and support from the

President and Secretary of Defense and can call on the expertise and technical support of all other designated supporting commands ~~designated supporting commands~~.

(1) ~~**Operations Officer (J-3).**~~ Combatant commanders normally **assign responsibility for IO within the operational area** to the ~~**Operations officer (**~~**J-3**~~)~~. When authorized, the director of the J-3 will have primary staff responsibility for planning, coordinating, and integrating joint force IO.

(2) **IO Officer.** ~~To assist the J-3 in exercising joint IO responsibilities, t~~**The J-3 normally will designate an IO officer** to assist in executing joint IO responsibilities. The IO officer is the central point of contact for IO on the combatant command staff. ~~This may entail ensuring representation of IO concerns within both operational and administrative processes of the staff (see paragraph 5 below), leading the IO portion of the J-3 staff, and/or directly facilitating coordination between internal and external components or staff organizations responsible for planning and execution of IO within the AOR and coordination with other AOR's through USSTRATCOM.~~ The primary function of the IO officer is to ensure that IO ~~is~~ are integrated and synchronized in all planning processes of the combatant command staff and that IO aspects of such processes are coordinated with higher echelon, adjacent, subordinate, and multinational staffs. In operational planning, the IO officer ensures that the IO portions of JOPES and ~~TSCP~~ theater security cooperation planning products reflect the combatant commander's guidance and are consistent with the operational principles and elements of operational art discussed in JP 3-0, *Doctrine for Joint Operations*, and Chapter V, "Planning and Coordination," of this publication. ~~information activities within an AOR/JOA~~. The IO officer normally is responsible for functions shown in Figure IV-1.

(3) **IO Staff.** The IO officer is normally assigned responsibility for supervision of IO activities for that portion of the J-3 staff designated as IO planners and ~~core capability~~ for the IO activity of the IO capable subject matter experts (SMEs) within the joint force. The portion of the staff under the cognizance of the IO officer is normally given a specific numerical designation such as "J-39." This staff section assists the IO officer and provides IO planning and core capability expertise within the staff and coordinates with ~~higher echelon, adjacent, subordinate, and multinational~~ other staffs and supporting agencies and organizations ~~as directed by the IO officer and/or established in staff SOPs. During the **planning phases** of an operation, the IO staff section should facilitate the planning efforts between various staffs, organizations, and parts of the JFC staff responsible for planning elements of IO.~~ During the **execution phase** of an operation, IO planners ~~should~~ shall be available to the joint operations center (JOC) or its equivalent to assist in integration, deconfliction, support, or adjustment of IO efforts as necessary. If IO manning permits and the J-3 or IO officer designates, **IO staff personnel may be part of the JOC watch team** or stand a separate watch ~~during the execution phase of an operation~~. Due to the sensitive nature of some aspects of IO, all members of the IO staff should have appropriate security clearance and access necessary to fulfill their IO responsibilities.

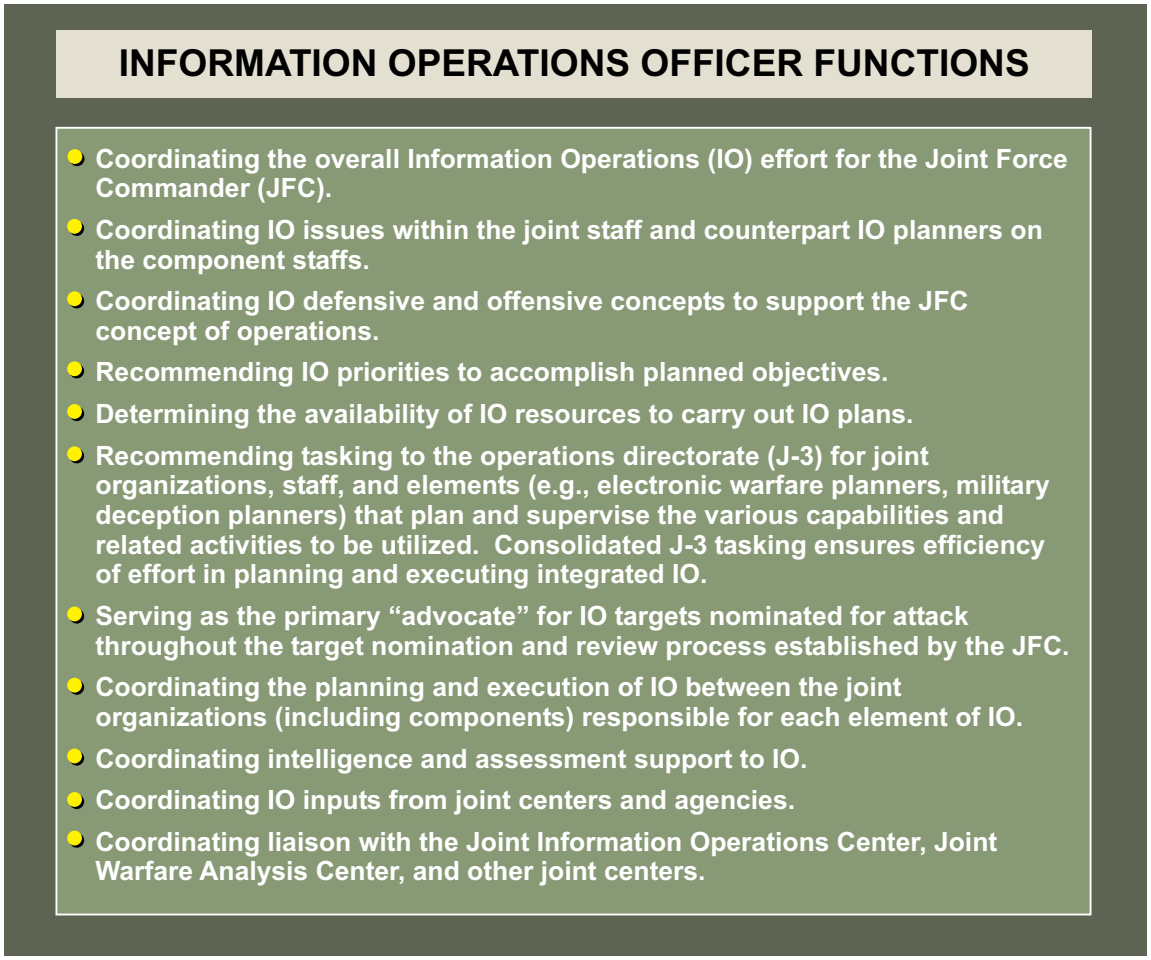


Figure IV-1. ~~Typical~~ Information Operations Officer Functions

(4) **IO Cell or Planning Organization.** To integrate and synchronize the core capabilities of IO with IO supporting and related capabilities and other staff functions handled by other portions of the staff, the IO officer normally leads an "IO Cell" or similarly named group as an integrated part of the staff's operational planning group or equivalent. ~~The also have planning processes.~~ The organizational relationships between the joint IO cell and ~~these~~ 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 both to the Service and functional components and to JFCs that have operational control of the forces. ~~**The size, structure, and planning methods used by these planning organizations vary widely.**~~ The specific duties and responsibilities of representatives from these supporting organizations should be established between the IO officer and the senior representative of each supporting organization. **Authorized staffing levels**, **mission**, and **location of JFC staff vis-à-vis each capability-level organization** are among the considerations that should be taken into account in determining how capability-level 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:

(a) **EW Representative.** ~~Provides **EW expertise and advocates EW interests and concerns** during IO cell planning deliberations.~~ Coordinates **EW activities and acts as**

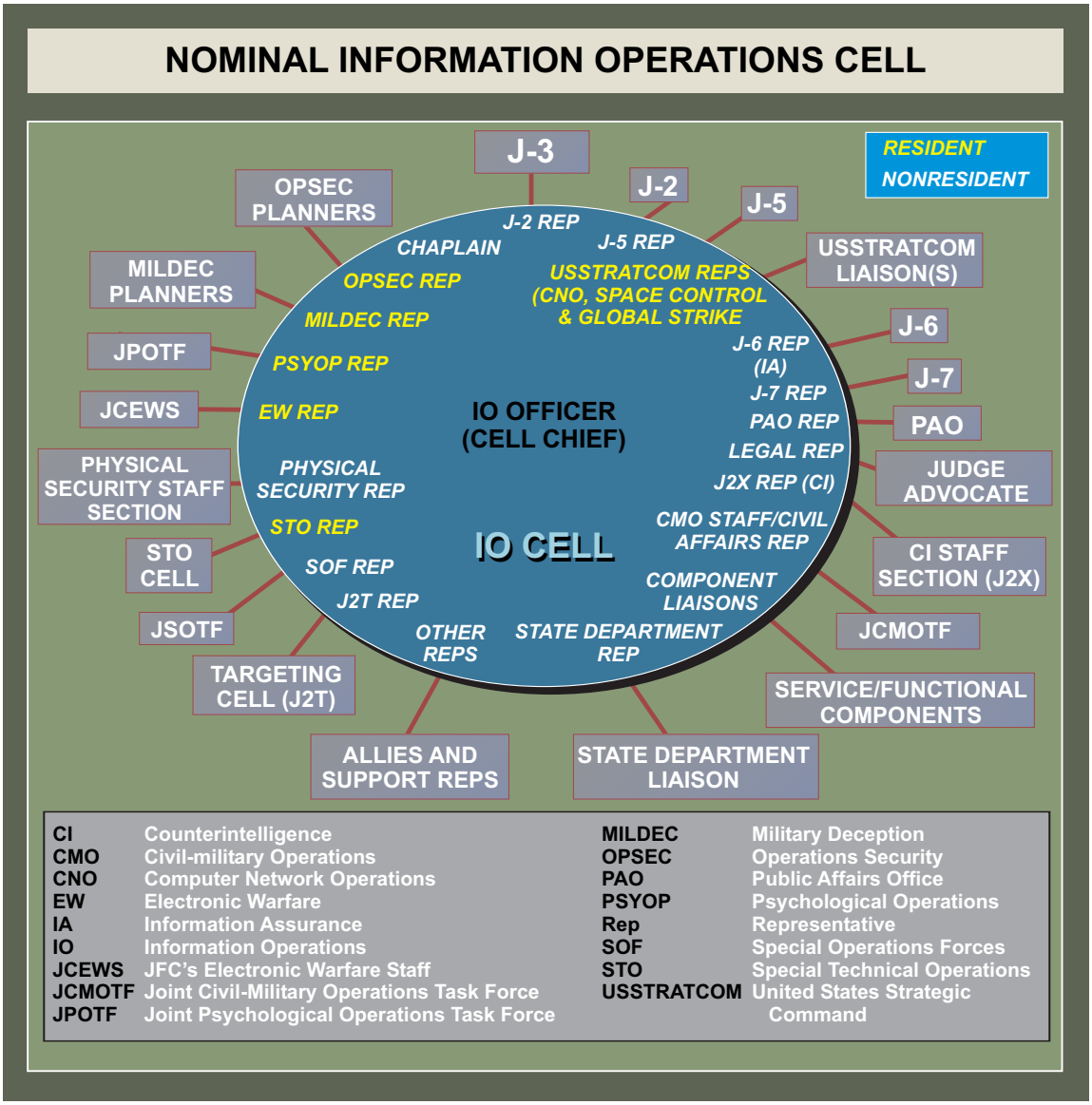


Figure IV-2. Nominal Information Operations Cell

liaison between the IO cell and the ~~EWCC~~ electronic warfare coordination cell (if formed). Serves as **Joint Spectrum Center (JSC) liaison officer** in the absence of an EWCC. If an EWCC is formed, the EWCC Chief or his designated representative will act as the IO representative. Coordinates closely with J-6 planner to deconflict friendly IO on the ~~communications~~ EM spectrum. Provides oversight of input and changes to the J~~F~~RFL.

(b) **CNA Representative.** Provides **CNA expertise and advocates CNA interests and concerns** during IO cell planning deliberations. Coordinates integration and synchronization of CNA with other IO capabilities and deconfliction of CNA with other staff directorates and organizations represented in the IO cell.

(c) **PSYOP Representative.** Provides PSYOP expertise **and advocates PSYOP interests and concerns** during IO cell planning deliberations. Develops PSYOP themes,

messages, and objectives. Provides military support to PD. Integrates, coordinates, deconflicts, 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 JPOTF and the in-theater multinational PSYOP cells, as appropriate.

(d) **OPSEC Representative.** Provides OPSEC expertise **and advocates** OPSEC **interests and concerns** during IO cell planning deliberations. ~~Coordinates combatant command or subordinate **joint force command OPSEC activities**.~~ Identifies critical information and existing vulnerabilities. Works with J-2 to develop EEFI. Develops OPSEC countermeasures. Serves as the Joint communications security (COMSEC) Monitoring Activity (JCMA) point of entry into the staff. Works closely with J-6 planner for COMSEC monitoring coordination~~JCMA liaison~~.

(e) **MILDEC Representative.** Provides MILDEC expertise **and advocates MILDEC interests and concerns** during IO cell planning deliberations. Coordinates combatant command or subordinate joint force command MILDEC planning.

(f) **Special Technical Operations (STO) Representative.** Provides STO expertise **and advocates STO interests and concerns** during IO cell planning deliberations. ~~The STO representative normally **coordinates Joint Warfare Analysis Center (JWAC) support and may coordinate JSC support**.~~ The STO planner should be an integral member of the IO cell to ensure STO planning is fully integrated and coordinated. STO read-ons are required throughout the IO staff.

(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) ~~**C4 (J-6) C4 IA Representative.**~~ Provides **IA to include CND expertise and advocates IA interests and concerns** during IO cell planning deliberations. Facilitates **IA and coordination** between information system planners and managers and members of the IO cell. Coordinates with the J-3 to **minimize offensive IO operations impact** on ~~own force~~ friendly forces C2. Principal liaison with the joint communications control center (JCCC). Identifies critical information systems and vulnerabilities of these systems and networks (Nonsecure Internet protocol Router Network, SECRET Internet Protocol Router Network [SIPRNET], Joint Worldwide Intelligence Communications System, voice, video, data, satellite, tactical comms). ~~**Coordinates information system support** to the IO cell. May serve as the Joint COMSEC Monitoring Activity (JCMA) point of entry into the staff.~~May assist coordination between the J-3 and OPSEC planners with JCMA for COMSEC Monitoring Activity.

(i) **J-2 Representative.** ~~Provides **intelligence process expertise and advocates J2 interests and concerns** during IO cell planning deliberations. Serves as the focal point for intelligence support to IO as discussed in Chapter IV, "Intelligence Support to IO."~~ Coordinates **collection requirements** and **analytical support** for compartmented and noncompartmented IO. May serve as liaison to the IO cell for Central Intelligence Agency, Defense Intelligence Agency (DIA), or NSA.

(j) **Targeting Cell Representative.** ~~Provides **targeting process expertise and advocates J2T interests and concerns** during IO cell planning deliberations.~~ Represents the **targeting cell(s)** and **coordinates IO targeting** with the Joint Targeting Coordination Board (JTCB), if designated.

(k) **CI Representative.** ~~Provides CI expertise **and advocates CI interests and concerns** during IO cell planning deliberations.~~ Coordinates **IO inputs to CI activities** which have significant roles in both offensive and defensive 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 ~~(JRTOC)~~ and the base defense operations center ~~(BDOC)~~ when appropriate.

(m) **Logistics Directorate of a Joint Staff (J-4) Representative.** Provides **logistics expertise and advocates J-4 interests and concerns** during IO cell planning deliberations. Coordinates and integrates **IO logistic considerations** into the deliberate 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~~s~~, the J-4 representative can assist IO cell members in tracking movement of IO capabilities and their logistic support to and from the supported AOR. The J-4 representative relays ~~Represents~~ IO planning guidance for OPSEC to other J-4 staff personnel~~.~~ and ~~P~~provides logistic policy guidance as appropriate.

(n) **J-5 Representative.** ~~Provides **policy and planning expertise and advocates J-5 interests and concerns** during IO cell planning deliberations.~~ Coordinates integration and synchronization of IO cell procedures and products into staff operational and theater security planning processes ~~as directed by the commander and established in staff SOPs~~.

(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~~M&S, and lessons learned interests and concerns** during IO cell planning deliberations. Serves as primary **integrator of IO into exercises and ~~modeling and simulation (~~M&S~~)~~**, especially at the JTF level. Ensures resulting lessons learned are incorporated into the **Joint ~~Universal~~ Lessons Learned Program ~~System (JULLS)~~**, as appropriate.

(p) **PA Representative.** Provides **PA expertise and advocates PA interests and concerns** during IO cell planning deliberations. Coordinates **and deconflicts PA activities with planned IO**.

(q) ~~J-9 (CMO)~~ **CMO Representative.** Provides **CMO expertise and advocates CMO interests and concerns** during IO cell planning deliberations. Ensures **consistency of CMO activities** within the JFC's AOR or joint operations area (JOA) that may support IO. Provides IO cell cultural advice and analysis of IO impacts on civil targets. Coordinates IO support to CMO as required. Provides interagency coordination with intergovernmental organizations, nongovernmental organizations (NGOs), and host nation. Provides feedback on IO MOE.

(r) ~~Staff~~ **Judge Advocate (~~S~~JA) Representative.** Provides **legal expertise and advocates ~~S~~JA interests and concerns** during IO cell planning deliberations. Advises planners to **ensure IO comply with domestic and international law** and assists with interagency coordination and negotiation.

(s) **Special Operations Representative.** Provides **~~S~~special ~~O~~operations expertise and advocates ~~S~~special ~~O~~operations interests and concerns** during IO cell planning deliberations. Coordinates **use of SOF** within a AOR or JOA in support of IO.

(t) **Service and Functional Component Representatives.** Provide **~~F~~functional ~~C~~component expertise and advocates Service and ~~F~~functional component interests and concerns** during IO cell planning deliberations. These officers, designated by the component commander~~,~~ or an assistant, will interface with the ~~joint force~~ combatant command IO cell to provide component expertise and act as a liaison for IO matters between the ~~joint force~~ 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 ~~JFC~~ 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) 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 theater and operational levels. Information may influence current strategy, planning, operations and execution in order to achieve theater objectives and support commanders. Commanders and their staffs may consider religion, cultural issues, and ideology when developing schemes of maneuver, ROE or planning CMOs, PSYOP, IO, and PA activities. Chaplains interacting with local religious leaders and NGOs can provide religious diplomacy and advise commanders on issues that could potentially alienate coalition partners and civilian populations and hamper military operations.

(~~u~~v) ~~Department of State (DoS~~DOS~~)~~ **Representative.** Provides **PD expertise and advocates PD and ~~DoS~~DOS interests and concerns** during IO cell planning deliberations.

(~~v~~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 ~~Information Operations~~ Guidance," (published separately), for additional organization guidance and responsibilities.

b. **~~JTF~~ Joint Task Force Command Organization~~.~~**

(1) Differences between JTF and combatant commander IO staffs are more a matter of scale than function. ~~The JTF's AOR and the scope of the JTF commander's mission(s) are normally smaller than those of a combatant commander.~~ While the scale of ~~AOR~~ JOA and scope of a JTF's mission may be smaller, the intensity of effort ~~and assigned~~ may require a larger IO staff than at the combatant command level. Level of effort, time constraints, mission, and operational variables are among the factors that may affect the specific manning requirements at the JTF level. ~~JTF's~~ JTFs may be permanently or temporarily stood up to accomplish specific missions. The size of the IO staff ~~on~~ 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 ~~Task~~ Force Headquarters (SJ~~T~~FHQ) ~~concept~~ prototype combines the training and organizational advantages of a permanent staff with the operational flexibility of a temporary JTF. The ~~SJTF~~ SJFHQ staff provides a core of expertise for all staff functions, including IO, ~~that~~ which is augmented as necessary for specific missions and ~~places~~ placed under the OPCON of the supported combatant commander. The ~~SJTF~~ SJFHQ SOP provides organization and functional procedural guidance across SJ~~T~~FHQ staff functions. The ~~SJTF~~ SJFHQ SOP includes guidance specific to IO. Copies of the ~~SJTF~~ SJFHQ SOP may be obtained through the United States Joint Forces Command (USJFCOM). USJFCOM points of contact are provided in Appendix C, "IO Support Points of Contact."

(2) The primary purpose of a JTF IO staff is to focus IO planning and support within the task force headquarters. As at the combatant command level, the JTF IO staff provides expertise to the other JTF headquarters (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 in JTF administrative and operational and execution phase (air tasking order [ATO] development etc.) processes ~~as~~ is discussed in paragraph 5 below and in Chapter V, "Planning and Coordination."

(c) Oversight of the IO aspects of 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 core, supporting, and related capabilities**. Support for IO comes primarily from within DOD, but other government agencies and organizations, as well as some allied agencies and organizations, may support the IO effort ~~through directly liaison with the joint staffs~~.

(1) Support from within DOD includes, but is not limited to, personnel augmentation from the **Service IO organizations, USSTRATCOM, United States Special Operations Command (USSOCOM), Joint Warfare Analysis Center (JWAC), Joint Information Operations Center, Joint Program Office for Special Technology Countermeasures (DPO)**, **JSC**, and **JCMA**. Additionally, through the various joint organizations that plan and direct ~~cure,~~ core, supporting, and related IO capabilities, **~~the IO~~ commanders and planners have access to the Service or functional component expertise** necessary to plan the employment or protection of Service or functional component systems or units. Service and functional components requesting specific IO support from sources internal or external to the joint force normally should request such support through the respective joint force component headquarters ~~to the combatant command IO staff~~.

(a) **National Security Agency.** NSA support for IO may be coordinated through the J-2 representative of the IO cell or directly from a NSA representative ~~according to procedures within each joint staff. NSA provides a variety of support to IO~~ including:

1. Information security (INFOSEC) technology, products, and services.

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

3. ~~Consultation and guidance for use in d~~Determining exploitation risk for telecommunications systems.

4. ~~Assistance with supporting and d~~Deconflicting national IO efforts with combatant command and JTF IO efforts.

5. ~~Assistance in d~~Determining release of COMSEC materials to allies or coalition partners.

~~6. Other assistance as described in Appendix A, "Supplemental Information Operations Guidance," (published separately) and Appendix C, "IO Support Points of Contact."~~

(b) **Defense Intelligence Agency.** DIA support for IO may be coordinated through the J-2 representative of the IO cell or directly ~~from a~~ with the DIA representative ~~according to procedures within each joint staff. DIA provides a variety of support to IO~~ including:

1. ~~Precise and timely i~~Intelligence for IO target selection and post-strike analysis.

~~2. Direct intelligence assistance in the planning and execution of defensive IO.~~

2. ~~Assistance in i~~Identifying friendly vulnerabilities and the most probable friendly targets within the adversary's ~~or potential adversary's~~ capabilities and concept of operations.

3. ~~Assistance in d~~Developing all-source intelligence gain/loss assessment of IO targets.

~~5. Other assistance as described in Appendix A, "Supplemental Information Operations Guidance." See also Appendix C, "IO Support Points of Contact."~~

(c) **Defense Information ~~Support~~ Systems Agency (DISA).** DISA support for IO may be coordinated through the J-6 representative of the IO cell or directly ~~from a~~ with the DISA representative ~~according to procedures within each joint staff. DISA provides a variety of support to IO including~~ and includes:

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

2. ~~Assistance~~ Assisting in disseminating ~~warnings of~~ adversarial CNA attack warnings.

3. Assisting in establishing a security architecture and standards for protecting and defending the ~~DII~~ GIG within the JOA.

~~4. Development of an information system incident program and a security incident response capability for protecting and defending the DII within the JOA.~~

~~5. Assessment of the vulnerabilities of information and information systems and development within available capabilities of procedures to mitigate assessed vulnerabilities and threat effects.~~

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

(d) **JWAC.** The JWAC assists ~~the Chairman of the Joint Chiefs of Staff and~~ the combatant commanders in their preparation and analysis of joint operation plans (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 will support a JTF through the supported combatant commander. See Appendix A, "Supplemental Guidance," ~~and Appendix~~ (published separately).

(e) ~~**Joint Program Office for Special Technology Countermeasures (JPO-STC**~~**DPO**~~**).**~~ The ~~JPO-STC~~ DPO provides the combatant commanders, ~~Military~~ Service Chiefs, and ~~DOD mission planners~~ operating forces with the **ability to assess their infrastructure dependencies and the potential impact on military operations** resulting from disruptions to key infrastructure components~~. Specific infrastructures addressed include~~ (i.e., electric power,

natural gas, liquid petroleum, transportation, and telecommunications ~~(Public Switched Network~~). ~~JPO STC~~ DPO also conducts **technical assessments of emerging special technologies** to determine their potential impacts to military and civilian systems and proposes countermeasure solutions and/or response options, as warranted. See Appendix A, "Supplemental Guidance~~,~~." ~~and Appendix C, "IO Support Points of Contact."~~

(f) **Joint Spectrum Center.** 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. ~~Assistance in development of the JRFL.~~ The JSC may deploy an augmentation team trained to prepare a JRFL or provide training and assistance in how to prepare a JRFL.

3. The JSC may deploy an augmentation team trained to prepare a JRFL to locate and identify interference sources and recommending 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. ~~The JSC may deploy teams capable of quickly locating and identifying interference sources and recommending technical and operational fixes to resolve identified interference sources.~~

5. Data about foreign C4 frequency and location data.

6. Unclassified C4 area studies about the regional C4 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.

(g) **Joint COMSEC Monitoring Activity.** The JCMA can provide the following direct support to the JFC through the IO cell~~:~~.

1. ~~Provides~~ INFOSEC monitoring and analysis support.

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

3. ~~Conducts c~~Cryptographic or plain language system monitoring.

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

(h) **Joint Communications Support Element (JCSE).** The JCSE provides **tactical communications support**, to include augmentation by a wide array of tactical and commercial communications equipment **for joint operations**.

(i) **Joint Communications Control Center.** JFCs normally establish a JCCC to **support ~~top level network control and management~~ network operations (NETOPS)** within the AOR or JOA. NETOPS is an organizational, procedural and technological construct for ensuring information superiority and enabling speed of command for the warfighter. NETOPS includes three primary functions: network management, information dissemination management, and IA. JCCCs play a vital role in IO, particularly in the IA process, where they provide **J-6 connectivity** throughout the chain of command. JCCC may incorporate the use of joint network management system which may include the joint defense infrastructure control system. These systems play a high-level network planning, monitoring and control system illustrating the network common operational picture that will be used combat operations.

~~1. Combatant Command. If established by the combatant command J-6, the JCCC provides a conduit for secure interoperability issues above and below the combatant command level. The JCCC can support the combatant command IO cell by coordinating with the J-6 to integrate various disciplines and capabilities associated with protecting and defending information and information systems.~~

~~2. When established at the JTF level JCCC provides the JTF IO cell with support similar to that provided by the combatant command JCCC (when established), to include serving as a conduit throughout the chain of command for secure interoperability and deconfliction issues.~~

~~(j) **Information Operations Technology Center (IOTC).** See Appendix A, "Supplemental Information Operations Guidance," (published separately)~~

(2) **Interagency Support.** Non-DOD USG departments and agencies may have a role in the planning and accomplishment of IO. The expertise, programs and activities of wide variety of non-DOD USG agencies should be **considered as part of the IO plan when appropriate**. JFCs establish staff procedures specific to their AOR for requesting interagency support and coordination of various aspects of joint operations through the interagency process as described in Volume I of JP 3-08, *Interagency Coordination During Joint Operations*. Normally joint commands work through designated liaison representatives attached to their command by various government organizations and agencies. 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 operation is discussed in Chapter V, "Planning and Coordination." The following Departments, agencies and organizations is not all inclusive but representative of possible interagency support and coordination required for IO.

(a) **Department of State.** (Placeholder for discussion of organization of Department of State coordination and support of IO, including coordination of PD). See Volume II of JP 3-08, *Interagency Coordination During Joint Operations*.

(b) (Placeholder IO support and representation from non-DOD intelligence community). See Volume II of JP 3-08, *Interagency Coordination During Joint Operations*. See also Appendix A, "Supplemental Guidance," (published separately).

(3) **Multinational Support.** Chapter VI, "Multinational Considerations in Information Operations," discusses multinational support of IO.

5. Joint Boards, Processes, and Products Related to ~~IO~~Information Operations

A broad array of staff functions may require coordination and deconfliction with IO. Staff functions required to plan and monitor joint operations are carried out through various processes, organizations, and products specified in joint doctrine, SOP, and other sources of guidance. Specifics of these processes, organizations, and functions are unique to each joint staff. ~~Figure VI-3 provides a table of joint staff processes, organizations, and products related to operational planning and execution which may require IO coordination or deconfliction.~~ The degree of interaction between IO and other staff functions during joint operations is situational and phase dependent. The IO officer or senior person responsible for IO, in consultation with other members of the staff, determines which internal organizations and processes to participate in and tracks IO integration and synchronization in those organizations, processes and products.

Intentionally Blank

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~~ Gen Anthony Zinni, CDR USCENTCOM
1997-2000

SECTION A. FUNDAMENTALS AND CONSIDERATIONS

1. Introduction

IO planning should follow the same principles, processes, and practices as traditional joint planning. IO provides capabilities in support of JFC missions in both a main and a supporting effort. Due to the inherent connectedness of the information environment, IO must be coordinated to the maximum extent possible with other USG information activities inside and outside of DOD through the interagency process. Uncoordinated IO can compromise, complicate, or negate other USG information efforts. Likewise, other USG information activities, when uncoordinated with DOD IO, may complicate or defeat DOD IO efforts or render them ineffective. IO are an approach that is contained in a plan. It is not EW, CNA, or managing perceptions. These are the tools of IO. Successful execution of an information strategy requires the effective synchronization and integration of these many tools associated with IO. This can **only** be done via a comprehensive plan. **This is the key to efficient and effective IO** — an all encompassing, integrated plan developed as early as possible from an information age viewpoint.

2. Information Operations Considerations in Joint Planning

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

b. IO planning, and often execution, 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.

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

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

coherent strategy by the establishment of agreed IO objectives as an integral part of the overall plan.

e. Establishing the organization of subordinate forces and designating command relationships ~~also~~ is very important in developing and executing IO. Establishing these relationships is the basis for achieving unity of command and effort among air, land, sea, space, and special operations forces. ~~This also establishes interagency agreement on the synchronization, coordination, and deconfliction process for IO planning and execution.~~

f. During IO planning, ~~for IO,~~ the planners will identify adversary vulnerabilities, devise required tasks and ~~sub-tasks~~ subtasks, and identify access (opportunities) and the means to exploit these vulnerabilities to achieve the JFC's objectives. The means or capabilities used by the JFC will vary from organic ~~non-compartmented~~ noncompartmented capabilities to national level capabilities. This requires the planners to identify Service, joint, and interagency IO capabilities available to the JFC for planning purposes, thereby providing a "toolbox" for the JFC to use in developing an IO plan and facilitating an effective capability-to-target match.

g. As part of the planning process, designation of release and execution authority is required. Designation of approval authority for some IO core capabilities will ~~may~~ be required. Release authority provides the approval for IO employment and normally specifies the allocation of specific offensive means and capabilities provided to the execution authority. Execution authority is ~~defined~~ described as the authority to ~~conduct~~ employ IO capabilities at a designated time and/or place. Normally, there is one execution authority within an operational area, designated in the execution order, which is the supported JFC.

h. IPB for IO differs from traditional requirements in that ~~they~~ it may ~~need~~ require greater lead time and may have expanded collection requirements. Chapter III, "Intelligence, Command, Control, Communications, and Computers Support to Information Operations," provides more information on intelligence considerations.

i. **Operational Preparation of the Battlespace (OPB).** OPB includes non-intelligence activities conducted to plan and prepare for potential follow-on military operations. OPB is conducted under Title 10 authority. Electronic IO benefits from, and often requires OPB for successful operation. IO OPB is divided into three areas.

(1) OPB-Orientation Activities (OA) provide familiarity with the operating environment. OPB-OA develop plans, information, and infrastructure that facilitate follow-on operations and operational readiness. Examples include gathering general operational information, blue force asset engagements in the operating environment, and C2 and BDA structure validation.

(2) OPB-Target Development is the collection of operational information on an identified/potential target for the purpose of acquiring/pinpointing the specific target, without engaging the target itself. Target information will be gathered and submitted in real time so that it remains current and relevant. Examples include verification of network structure and access with operations tools or weapons.

(3) OPB-Preliminary Engagement of the identified/potential target is used to find and fix, track and monitor, or otherwise influence target operations, which precede the main effect. Examples include engaging the target to verify TTP, identify and/or drive the adversary to alternate modes of target operation, and conditioning adversary forces.

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

j. **Legal Consideration in IO. IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval.** The United States has constitutional safeguards, laws, and legal procedures to set boundaries and establish precedence for military activity in the information ~~dimension~~ environment. Other countries legal basis for military activity in the information ~~dimension~~ environment may differ. Beyond strict compliance with legalities, conduct of United States military activities in the information ~~dimension~~ environment as in the physical ~~dimensions~~ domains, are conducted as a matter of policy and societal values on a basis of respect for fundamental human rights. United States forces, whether operating physically from bases or locations overseas or virtually in the information ~~dimension~~ environment from within the boundaries of the United States or elsewhere, are required by law and policy to act in accordance with United States law and the ~~law of armed conflict (~~LOAC~~)~~.

(1) Legal limitations may be placed on IO ~~across the range of military operations~~. All military activities in the information ~~dimension~~ environment should be assumed to be subject to the LOAC. ~~**If there is any question of the legality of particular IO tasks,**~~ **In order to determine whether there are any questions of the legality of particular IO tasks, such tasks ~~should~~ must be reviewed by the appropriate ~~S~~JA and approved by appropriate levels of the chain of command.** Bilateral defense treaties to which the United States is a signatory may have agreements concerning the conduct of IO ~~or one or more of its core,~~ and its supporting, or related capabilities. Use of IO also may be regulated under status-of-forces agreements. A current list of treaties and other international agreements in force is found in Department of State Publication 9434, *Treaties In Force*.

(2) Some aspects of IO, such as ~~information~~ fires in the information environment, may be considered hostile acts by other countries. ~~when and other aspects of IO and between IO and other military information activities.~~

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

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

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

(c) Structure and relationships among United States intelligence organizations and ~~general interagency relationships,~~ the overall interagency environment, including NGOs.

k. IO planners must avoid projecting US value sets on opponents (mirror imaging). Therefore, incorporating specific country experts into the IO planning process will help prevent developing plans based on inaccurate cultural influences.

3. Division of Planning Labor

IO Cell. At the combatant and subordinate joint force command levels, the **IO cell is the focal point for IO planning**, to include integration, synchronization, coordination and deconfliction. ~~The IO cell should **exchange information with cell members** about plans in development.~~ The IO cell should focus on **integration** and **deconfliction** of capabilities to accomplish mission objectives. **The IO cell should be an integral part of all joint force planning activities.** The specific procedures of how the IO cell is integrated into planning activities is command specific. ~~Members of the IO cell may represent IO cell interests and concerns in other meetings or planning processes within JOPES or TSCP. Figure VI () in Chapter VI, "Responsibilities and Command Relationships," provides a nominal list of staff processes and organizations that may require IO coordination.~~ Key joint staff planning organizations that require IO representation include:

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

b. **Joint Target~~ing~~ Coordination Board.** The IO cell provides representation to the JTCB~~, if designated, can provide **the conduit for ensuring effective IO coordination** and normally will provide a means to coordinate joint force capabilities with the application of IO and other conventional operations~~ for effects-based targeting in accordance with JP 3-60, *Joint Doctrine for Targeting*.

4. Integration and Synchronization

a. ~~Integration is the arrangement of military forces and their actions to create a force that operates by engaging as a whole. Synchronization is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time.~~ During ~~joint~~ planning ~~processes,~~ IO capabilities and their uses are considered and their use integrated and synchronized ~~according to established TTP and/or principles of war/MOOTW (see JP 3-0, *Joint Doctrine for Operations*) and the elements of operational art, to accomplish specific planned tasks and achieve planned IO objectives~~ with other JFC resources. IO capabilities are collectively integrated and synchronized with other military activities in the physical ~~dimensions (see discussion of dimensions in Chapter I, "Introduction")~~ domains to achieve ~~broader~~ operational objectives. One of the most critical aspects of integrating and

synchronizing IO with other operations ~~in the physical dimension~~ is the integration of ~~information fires with other types of joint~~ fires.

b. **Fires Integration**

(1) The JFC is responsible for ensuring the integration and synchronization of fires. Synchronization, integration, allocation of resources, and matching appropriate lethal and ~~non-lethal~~ nonlethal fires to particular targets are functions of the component commanders. When ROE allow ~~information~~ fires ~~(see discussion of information fires in Chapter I, "Introduction"),~~ in the information environment, they must be integrated and synchronized with other types of joint fires ~~as discussed in JP 3-09, *Joint Doctrine for Fire Support Operations*~~. IO core capabilities provide the primary means joint forces use to provide ~~information~~ fires in the information environment. ~~Information fires of land, air, sea, and special operations forces, along with space, and multinational assets when appropriate, are integrated to maximize the effectiveness of joint fires. Information and information infrastructures are targeted by IO assets of the various components to support joint operations.~~ Because of the global nature of the information environment, fires in the information environment should be integrated and synchronized on a larger scale depending on the intended fires in the information environment to be conducted.

(2) **Supported and Supporting Relationships.** ~~Because of the potential global reach of electronic, space, and cyber information fires, the need to integrate synchronize fires efforts must now be carried out on a global scale.~~ At each command level, from strategic through tactical, supported and supporting relationships may be established by the appropriate level JFC. ~~a specific commander is designated the supported commanders for a specific operation.~~ ~~**In the information dimension, all commanders at all levels are potential supporting commanders for every mission and every operation.**~~ ~~Within their designated AOR,~~ A designated supported commander~~s~~ synchronize~~s~~ ~~information fires with other~~ information activities and ~~with other~~ joint fires. I~~nformation f~~Fires ~~may~~ delivered from or into areas outside the supported commander's AOR, ~~is~~ are coordinated as directed by the next higher echelon of the chain of command.

(3) **Unity of Effort.** Because of the seamless nature of the information ~~dimension~~ environment, information efforts carried out within specific ~~command or AOs~~ AORs must be coordinated with strategic, inter-theater, and theater-wide information efforts ~~is critical~~ to avoid collateral damage to information ~~effects that may reverberate to 2nd, 3rd, and subsequent order of effects~~ systems up and down the levels of command. Planning, execution, and target acquisition ~~(TA)~~ capabilities often overlap. **Each JFC must ensure unity of effort throughout their own command and ensure that their ~~information~~ fires in the information environment are integrated and synchronized with other commands (on a global scale if necessary).** To facilitate synchronization, each JFC establishes priorities that will be executed throughout the AOR. ~~In coordination with the supported commander, those commanders designated by the JFC to execute theater- and/or JOA-wide functions have the latitude to plan and execute these JFC prioritized operations and attack targets within land and naval AOs.~~

5. Coordination and Deconfliction

~~IO encompass t~~The coordination and deconfliction of IO with all military ~~activity~~ activities in the information ~~dimension~~ environment in all types of operations is essential. ~~The implications of the scope of this task are that IO requires coordination and deconfliction functionally and organizationally.~~ This section discusses each of the types of coordination and deconfliction and provides basic guidance along with references where to find specific procedural guidance. In joint operations, JOPES planning processes are the primary methodology to coordinate IO functionally and organizationally. **The IO cell is the primary staff organization to accomplish IO coordination and deconfliction.**

a. **Coordination.** ~~In the context of this publication, it is the practical administrative or staff actions required to properly integrate and synchronize the component parts of a specific task to achieve the intended effects and contribute to the attainment of objectives.~~ Lack of ~~coordination~~ or improper coordination may reduce the ~~effectives~~ effectiveness of component parts or lead to unintended or negative effects. Avoidance of known combinations and sequences that have undesirable effects requires deconfliction and is described in paragraph 5.b. below. Coordination can be accomplished through individual or collective meetings, phone or radio conversations, email or recorded messages or through established staffing processes. ~~The~~ JOPES provides the formal structure for coordination in joint planning. Various processes that take place during the JOPES planning process provide for formal coordination of major aspects (intelligence, targeting, fire support, etc.) of joint operations. In joint operations, coordination occurs at multiple levels and from multiple perspectives. The individual capabilities of IO ~~is~~ are coordinated to achieve ~~planned integrated and synchronized effect to accomplish~~ specific objectives.~~,~~ IO ~~is~~ are coordinated with the other basic information functions ~~(see Chapter I, "Introduction")~~ to gain and maintain information superiority at various levels (tactical, operational, ~~theater,~~ strategic).~~,~~ IO ~~is~~ are coordinated with military ~~activity~~ activities ~~of~~ in the physical ~~dimensions~~ domains to achieve integration and synchronization ~~as planned~~ in joint operations. The six basic information functions of all ~~UGS~~ USG ~~activity~~ activities comprise the informational ~~element~~ instrument of national power that must be coordinated with other ~~elements~~ instruments of national power to achieve national security objectives. Key aspects of joint planning coordination relevant to IO include:

(1) **Staff IO Coordination Roles**

(a) **IO Staff Section.** The IO staff section~~, discussed in Chapter VI, "Responsibilities and Command Relationships,"~~ is the focal point of IO planning activity ~~for joint planning~~. The IO staff may be augmented during major planning projects by expertise from various IO supporting organizations. The IO staff coordinates as required and conducts IO-specific analysis ~~in support of planning and~~ to develop ~~the sections of~~ required planning products ~~assigned to the IO officer~~. ~~Each core capability staff section coordinates the internal aspects of their capability among themselves and with the other core capabilities staff sections as required to integrate and synchronize the five core capabilities. The IO staff coordinates with IO staff sections at senior, component, and multinational staffs as necessary to carry out planning processes and other duties.~~

(b) **IO Cell.** The IO cell, under the direction of the IO officer, provides the best entity for coordinating and ~~deconfliction~~ deconflicting of IO issues and concerns across staff

functions, command levels, USG support organizations, and allies and coalition partners. All core, supporting, and related capabilities, along with components, key staff functions, and supporting organizations are normally represented in joint IO cells. ~~The IO staff use meetings of the IO cell or meet with individual members informally to coordinate and deconflict IO issues among staff directorates, sections, other command levels, supporting organizations, and multination units.~~ The IO staff coordinates and deconflicts IO issues among staff directorates, command levels, and supporting organizations through the use of both formal and informal meetings. During major planning efforts, the IO cell becomes part of the ~~joint planning group (~~JPG~~)~~, or other higher level planning organizations ~~when~~ as appropriate.

(c) **Joint Planning Group. JFCs normally establish a JPG**, particularly at the JTF level. If a JPG is established, **the IO staff and cell must be an integral part of** the JPG's planning activities. Early and continuous exchange of information of planning activities between the JPG and the IO staff and cell is the key to close coordination. The IO staff completes planning tasks through coordination with the other IO cell members, provides IO perspectives in wider group discussions, and delivers IO and capability specific planning products and analysis to the JPG as required during the planning process.

(2) **Staff Functional Coordination.** Key staff functions that require close coordination with IO and not discussed previously ~~in Chapter III, "Supporting and Related Capabilities," Chapter IV, "Intelligence Support to Information Operations," or Chapter V, "Command, Control, Communications, and Computer System Support to Information Operations,"~~ include:

(a) **Targeting Coordination.** The ~~J2T~~ intelligence targeting community may designate a representative to participate in IO cell deliberations and provide joint targeting ~~process~~ expertise~~, as discussed in Chapter VI, "Responsibilities and Command Relationships."~~ Information ~~fires~~ operations may be employed against a variety of targets in both the physical and information ~~dimensions to achieve operational objectives~~ environments. Functional components conduct, coordinate and deconflict their own targeting with other components through the joint targeting process. Lethal and ~~non-lethal~~ nonlethal ~~kinetic~~ fires may be employed against physical targets to support IO objectives. The IO officer supervises the coordination of IO planning with target planning. Personnel with targeting expertise specific to IO ~~assigned to the IO staff (either permanently or temporarily) normally are~~ should be continuously involved in ~~representing~~ raising IO issues and concerns in the targeting process ~~during both the planning and execution phases of an operation~~.

See JP 3-60, Joint Doctrine for Targeting*, and JP 2-01.1,* Joint Tactics, Techniques and Procedures for Intelligence Support to Targeting*, for detailed discussion of joint targeting and associated intelligence support doctrine.*

(b) **Joint Fire Support Coordination.** ~~The concept of j~~Joint fire support is defined as joint fires that assist air, land, maritime, amphibious, information, and special operations forces to move, maneuver, and control territory, populations, airspace, and key waters. ~~Joint fire support is usually executed within the boundaries of the land, maritime, or amphibious force.~~ During ~~the~~ planning, commanders develop the scheme of maneuver and

concept for fires. ~~Commanders determine how to shape the battlefield with fires to assist maneuver and how to use maneuver to exploit the use of fires.~~ The Army and Marine Corps use two interrelated processes to enhance joint fire support planning and interface with the joint targeting process. The first is the decide, detect, deliver, and assess ~~(D3A)~~ process ~~and~~ which incorporates the same fundamental functions of the joint targeting process. The second process is the use of wargaming, which is an exercise performed by commanders and staffs to determine the best COA for a given operation. IO planners should be prepared to coordinate IO planning with either of these processes within the targeting planning process.

See JP 3-09, Doctrine for Joint Fire Support*, for detailed discussion of joint fire support and associated planning processes.*

(3) **Interagency Coordination.** IO coordination with USG components is required for consistency of IO informational themes with broader USG information themes and for support of IO from USG organizations outside ~~the~~ DOD. Identifying friendly information priorities requires close coordination and cooperation between DOD, other USG departments and agencies, and industry. Protection of the information infrastructure and friendly decision-making processes requires collaborative efforts to implement protective measures commensurate with the value of the information or information systems protected. Adherence to a common level of protection requires determining the scope of the protection effort needed in order to determine how much protection is needed. The synchronization and integration of the IO with other USG efforts requires clear national strategic guidance. ~~Volume I of JP 3-08, *Interagency Coordination During Joint Operations*, describes the interagency process.~~

For more information on interagency coordination, see JP 3-08, Interagency Coordination During Joint Operations, Vol. I.

(4) **Multinational Coordination.** See discussion in Chapter VI, "Multinational Considerations in Information Operations."

b. **Deconfliction.** ~~The process of coordination among organizations or their subdivisions to avoid incompatibility, irreconcilability, or opposition when two or more military forces or capabilities are employed simultaneously or in particular sequence during military operations.~~ **IO, like other aspects of operations, may require deconfliction at several levels.** ~~, i.e., within, above, and below the joint force, and at several levels of war.~~ In addition, **offensive and defensive IO may need to be deconflicted at the same level**. As with integration, deconfliction of IO should begin at the earliest possible stage of IO planning. IO ~~deconflicted~~ deconfliction should be a **continuous process** ~~which~~ that allows for **flexible phasing** of IO employment options. The likelihood of simultaneous IO at all levels of war and command is quite high. Additionally, the relatively large number of potential capability providers in the same ~~AOR or JOA~~ operational area, particularly when IO are a main element of a JFC's operations, makes **early identification of IO deconfliction issues essential**.

SECTION B. PLANNING PROCESSES

6. Introduction

~~There are four joint planning processes.~~ Military planning includes four broad types of planning: joint strategic planning, theater security cooperation planning, joint operation planning, and force planning. **Theater Security Cooperation Plans** (previously known as Theater Engagement Plans) are developed at the combatant command level. OPLANs, operation~~s~~ plans in concept format (CONPLANs) and operation~~s~~ orders (OPORDs) are ~~part of~~ created in the JOPES through ~~campaign,~~ the deliberate~~,~~ or crisis action planning process~~es~~. **IO plans should be developed ~~in support of~~ as an integral part of the JFC's overall planning effort.** To accomplish this, **IO planning should ~~occur simultaneously with~~ be seamlessly integrated into theater level planning or operational planning**. This requires IO staff to be represented at, and have a voice in, all elements of the planning process. This section discusses IO planning as a part of the processes used at joint commands to develop TSCPs, OPLANs, CONPLANs, and OPORDs. The section also describes the Joint IO Planning Process (JIOPP) that facilitates IO planning in JOPES planning processes.

7. Theater Security Cooperation Planning

a. A TSCP is ~~primarily~~ a strategic planning document intended to link combatant command-planned regional engagement activities with national strategic objectives. The TSCP is based on planning guidance provided in ~~the~~ CJCSI 3110.01E, *Joint Strategic Capabilities Plan ~~(JSCP)~~*, Enclosure E, "Engagement Planning Guidance." Combatant commanders plan and support operations and activities that produce multiple benefits in readiness, modernization, and engagement. However, peacetime military engagement activities must be prioritized to ensure efforts are focused on those that are of greatest importance, without sacrificing warfighting capability. TSCP identifies the synchronization of these activities on a regional basis and illustrates the efficiencies gained from ~~regional~~ geographic combatant command engagement activities that support national strategic objectives.

b. Combatant commanders and designated ~~E~~executive ~~A~~agents prepare TSCPs in accordance with procedures contained in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3113.01A, *Theater Engagement Planning*, and the format provided in Enclosure C, "Format and Content of Theater Engagement Plans," of that manual. TSCPs may be developed using the JOPES deliberate planning process as described below. TSCPs are submitted to the CJCS for review in accordance with CJCSI 3113.01, *Responsibilities for the Management and Review of Theater Engagement Plans*.

c. IO planning is as integral to TSCP development as it is ~~integral~~ to the JOPES-planning process. In TSCP development, combatant command ~~IO~~ planners analyze and plan how core~~,~~ supporting, and related capabilities can be integrated and employed at the theater level to support national interests in the AOR. Combatant commanders and designated ~~E~~executive ~~A~~agents plan strategic communications and military support to public diplomacy through the TSCP. In support of geographic combatant commanders, CDRUSSTRATCOM ~~coordinates~~ assists with coordination of IO portions of TSCPs across theater AOR boundaries.

8. Campaign Planning

~~a. A joint campaign is the synchronization of military operations in all dimensions with other USG diplomatic, economic, and information efforts to attain national and multinational objectives. While facilitated by such procedures as the JOPES and commonly accepted military decision making models, the operational design process is primarily an intellectual exercise based on experience and judgment. The key elements of operational design are: (1) understanding the strategic guidance (determining the desired end state and military objectives(s)); (2) identifying the critical factors (principal adversary strengths, including the strategic centers of gravity (COGs), and weaknesses); and (3) developing an operational concept or scheme that will achieve the strategic objective(s).~~ Planning for employment of IO in campaign planning begins with articulating and understanding the commander's mission, concept of operations, **objectives**, and **intent**. The same **fundamentals of campaign planning** shown in Figure V-1, apply to the IO portion of a campaign plan.

See JP 5-00.1, Joint Doctrine for Campaign Planning*, for more detailed discussion of campaign planning.* ~~*Annex D, "Location of Information Operations Guidance in JOPES Formats," to Appendix C, "Information Operations in JOPES Planning Processes," provides guidance for different sections of campaign planning products that pertain to IO or that should be coordinated and deconflicted with IO guidance.*~~ *See also Appendix A, "Supplemental Guidance," (published separately).*

9. Deliberate Planning

Each command modifies the deliberate planning process as needed. Discussion here is focused on how a combatant command IO staff might participate in deliberate planning. Staff actions mentioned are nominal and should be adapted and added to as each planning project requires. Figure V-2, provides a **general guide to IO planning** as an integrated part of the deliberate planning process at the combatant command level. Figure V-2 may be adapted for planning at the subordinate joint force and component levels as required.

a. **Phase I Initiation.**

(1) **Integration of IO into joint operations should begin at the initiation of planning.** Upon receipt of a new mission, either from the higher ~~headquarters~~ HQ or from the JFC, the commander and staff conduct an initial assessment.

(2) Key IO staff actions during the ~~I~~initiation ~~P~~phase include:

(a) **Review orders or other documentation that initiated planning.**

(b) **Meet with senior staff and JFC as necessary to advise on JFC's initial guidance.**

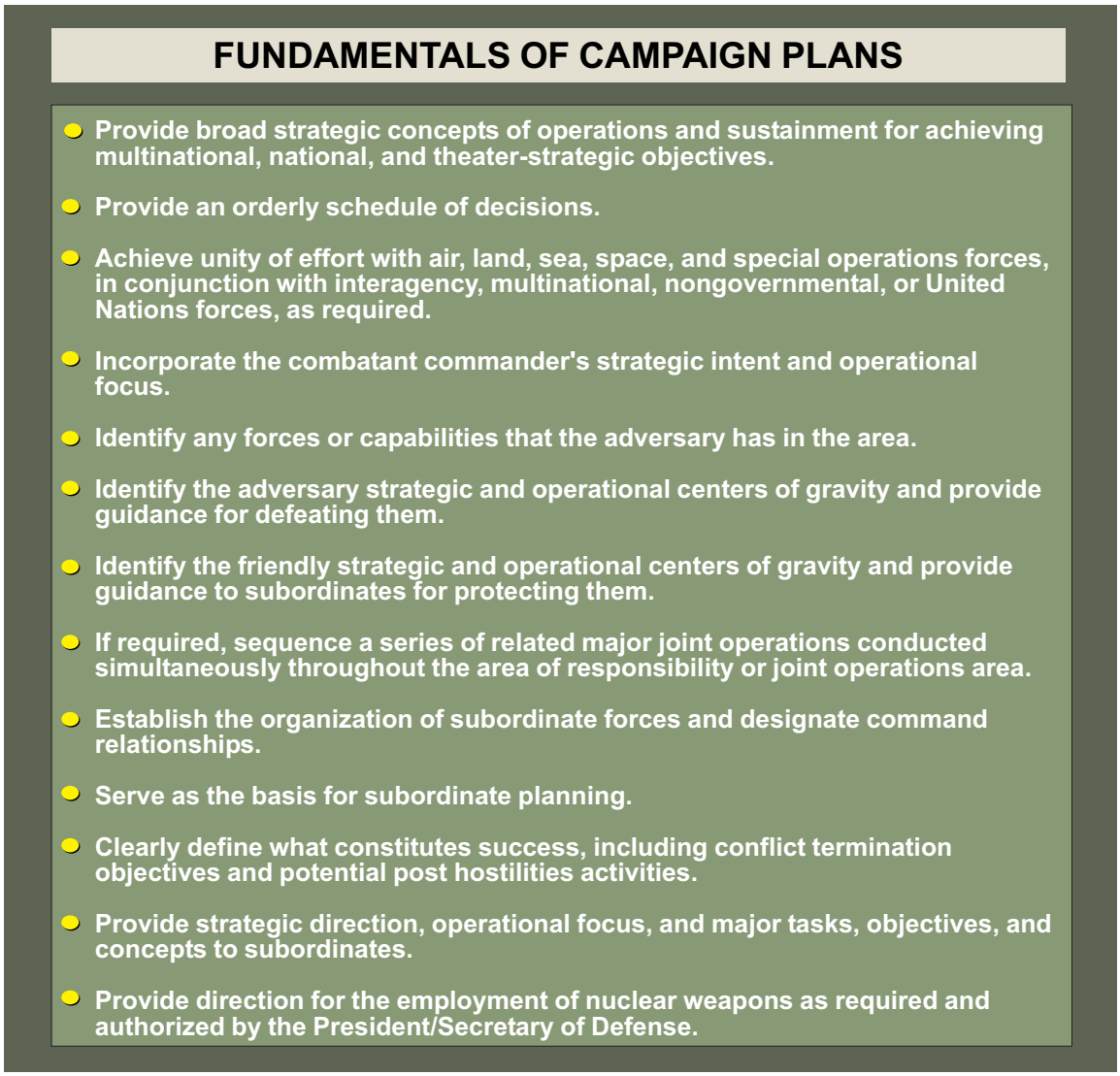


Figure V-1. Fundamentals of Campaign Planning

(c) ~~**IO officer and selected core capability staff d**~~**Discuss the JFC's initial guidance.**

(d) **Convene meeting of full IO cell or consult informally with other members as needed.** (Continues throughout deliberate planning process.)

(e) **Gauge initial scope of IO's role in the operation.**

1

INFORMATION OPERATIONS PLANNING RELATED TO DELIBERATE PLANNING

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

CJCS Chairman of the Joint Chiefs of Staff
IO Information Operations
JOPES Joint Operation Planning and Execution System
TPFDD Time-Phased Force and Deployment Data

Figure V-2. Information Operations Planning Related to Deliberate Planning

(f) **Obtain internal planning timeline from senior staff and any changes to local planning SOP battle rhythm** that will be specific to current planning effort.

(g) **Identify location and battle rhythm of other staff organizations that require IO interaction** and divide responsibilities for attendance among IO staff if not self evident.

(h) **Begin identifying information needed for concept development and availability of required information.** Continues through support plan development in deliberate planning.

(i) **Identify 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 (refine during concept development phase of deliberate planning).

(j) **Initiate ~~P~~priority ~~I~~intelligence ~~R~~requirements (PIRs)~~s~~, ~~R~~requests for ~~I~~information (RFIs), and other information requirements** to ~~obtain~~ update incomplete or outdated information required (continues throughout deliberate planning process) ~~(See Chapter IV, "Intelligence Support to Information Operations," for intelligence considerations in IO planning)~~.

(k) **Provide IO input to the warning order.**

~~*See Tab 1, "Initiation Phase," to Annex B, "Deliberate Planning Process," of Appendix E, "Information Operations in JOPES Planning Processes," for more detailed discussion about IO in this phase of the deliberate planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

b. **Phase II Concept Development.**

(1) **Mission Analysis.**

(a) The purpose of mission analysis is to analyze assigned tasks in order to determine the mission and to prepare guidance for subordinate elements. The JIOPP, discussed later in this chapter, begins here and runs in parallel with the deliberate planning process.

(b) Key IO staff actions during mission analysis include:

1. **Continue IO review** of any Joint Chiefs of Staff guidelines provided in the Joint Strategic Capabilities Plan (or other initiating guidance) begun in the ~~I~~initiation ~~P~~phase as part of JPG guidance review.

a. **Identify specified IO tasks** and provide to the JPG's compilation of specified tasks.

b. **Identify IO implied tasks** not specifically~~,~~ stated, but which must be completed to accomplish the stated mission and provide to the JPG's compilation of implied tasks.

c. **Identify assumptions, constraints, and ~~restraints~~ restrictions relevant to IO** and provide to the JPG's compilation of assumptions, constraints, and ~~restraints~~ restrictions.

2. **Analyze friendly forces IO capabilities** apportioned for the mission in support of JPG analysis of friendly force apportionment.

3. **Identify relevant physical, electronic, and human factor properties** (whether friendly, adversarial or neutral/third party) of the information ~~dimension~~ environment that may impact the operation. This analysis should include identification of informational aspect of adversary and friendly centers of gravity, critical (vulnerability, accessibility, and feasibility) aspects of relevant friendly and adversary decision-making processes broken down by quality criteria discussed in Chapter I, "Introduction." Provide completed analysis to JPG's overall mission analysis effort.

4. **Develop proposed PIRs and RFIs** ~~to required~~ to complete analysis of the information ~~dimension~~ environment and support IO planning.

5. **Provide IO perspective in JPG's development of restated mission and commander's mission objectives** for the combatant commander's approval.

~~*See Tab 2, "Concept Development – Mission Analysis," to Annex B, "Deliberate Planning Process," of Appendix E, "Information Operations in JOPES Planning Processes," for more detailed discussion about IO in the mission analysis step of concept development during deliberate planning. See also discussion of IO objective development in paragraph below and Appendix G, "Current Information Operations Planning Methodologies, Support Systems, and Tools." See also Appendix A, "Supplemental Guidance," (published separately).*~~

(2) **Planning Guidance.**

(a) The purpose of the planning guidance step is to inform all participants of the restated mission and combatant commander's objective(s), to issue any specific planning guidance from the combatant commander, and to begin development of possible ~~courses of action~~ COAs to accomplish the mission. A minimum of three proposed ~~courses of action~~ COAs are normally developed in deliberate planning. The commander may specify one or more ~~courses of action~~ COAs that he wants the staff to develop.

(b) Key IO staff actions related to planning guidance include:

1. **Assist initial drafting of commander's planning guidance** as requested.

2. **Propose revision of draft commander's planning guidance to reflect IO concerns or issues** during staffing.

3. **Contribute IO perspective to development of proposed COAs** by JPG.

4. **Develop proposed IO objectives and ~~sub-objectives~~ subobjectives.**

5. **Assist in development of commander's informational themes.**

~~*See Tab 3, "Concept Development – Planning Guidance," to Annex B, "Deliberate Planning Process," of Appendix E, "Information Operations in JOPES Planning Processes," for more detailed discussion about IO in the planning guidance step of the deliberate planning process. See also discussion of IO in commander's intent/guidance and IO objective development in paragraph below, Appendix G, "Current Information Operations Planning Methodologies, Support Systems, and Tools," and Appendix A, "Supplemental Guidance," (published separately).*~~

(3) **Staff Estimates.**

(a) The purpose of the ~~planning guidance~~ staff estimate step is to compare~~s~~ and contrast~~s~~ each proposed ~~course of action~~ COA and prioritize the ~~courses of action~~ COAs from most supportable to least supportable. The commander or J-3 may specify the degree of elaboration or particular details required in various staff estimates, including the IO estimate.

(b) Key IO staff actions related to staff estimates include:

1. **Review the mission and situation from an IO perspective** using the draft IO objectives/sub-objectives as the planning reference, to include placing the mission in the context of the information ~~dimension~~ environment analysis begun during mission analysis and refined as responses to PIRs and RFIs ~~are~~ received.

2. **Analyze each COA** from its staff functional perspective.

a. **Compare each COA based on IO mission analysis.** Include consideration of how well IO MOEs may provide feedback during each COA.

b. **Coordinate IO COA analysis with other relevant staff estimates,** particularly those that may place requirements on IO core, supporting and related capabilities.

c. **Prioritize COAs from the IO perspective.**

3. **Support development of IO portions of other staff estimates** as required.

4. **Provide prioritized IO estimates** to JPG.

~~See *Tab A, "Concept Development – Staff Estimates,"* to *Annex B, "Deliberate Planning Process,"* of *Appendix E, "Information Operations in JOPES Planning Processes,"* for more detailed discussion about IO in the staff estimates step of the deliberate planning process. See also discussion of IO measures of effectiveness in paragraph of *Section C* below and *Appendix A, "Supplemental Guidance" (published separately).*~~

(4) **Commander's Estimate.**

(a) The purpose of the commander's estimate is to formally compare the proposed ~~courses of actions~~ COAs by means of a decision briefing to the commander. At the end of the decision briefing, the commander is asked to select a ~~course of action~~ COA for which the staff will proceed to develop. The commander may select one of the proposed ~~courses of action~~ COAs as is, select a ~~course of action~~ COA with modifications, or choose an entirely different ~~course of action~~ COA.

(b) Key IO staff actions related to the commander's estimate include:

1. **Brief IO portions of each COA** to the commander ~~and answer questions as required~~.

2. **Revise IO portion(s) of selected COA as required** to develop the approved commander's estimate.

~~*See Tab A, "Concept Development – Commander's Estimate," to Annex B, "Deliberate Planning Process, of Appendix E," for more detailed discussion about IO in this step of the deliberate planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

(5) **Combatant Commander's Concept.**

(a) The purpose of this step is to formally develop and distribute the ~~C~~combatant ~~C~~commander's ~~course of action~~ COA selection and further guidance to all participants in the planning process. PA and PSYOP themes to be used in ~~for~~ each phase of the operation will have been developed in concert with the overall IO objectives and themes and should be included in such guidance. Appropriate levels of coordination will be obtained for all PSYOP themes. The PSYOP staff or component JPOTF has responsibility for development of PSYOP themes and ~~coordination~~coordinates/deconflicts with other members of the IO cell. The PA staff has responsibility for PA themes and ~~coordinates/deconflicts with other members of the IO cell~~ develops them in accordance with the commander's agreed IO objectives for each selected COA.

(b) Key IO staff actions related to the ~~C~~combatant ~~C~~commander's ~~C~~concept include:

1. **Prioritize IO objectives and sub-objectives** by phase of operations for selected COA.

2. **Select IO core, supporting, and related capabilities** that may be used individually or in combination (integrated and synchronized) to achieve IO sub-objectives developed previously. Begin development of **synchronization matrix** (see Figure VII-3) to assist in tracking capability employment. Capabilities selected should be based on the following considerations:

a. **Suitability** for use against identified critical aspects of adversary and friendly decision-making processes (from mission analysis step) based on operational principles from JP 3-0, 10 September 2001, ~~*Joint*~~ *Doctrine for Joint Operations*, and elements of the art of IO discussed later in this chapter.

b. **Availability** for IO tasking (based on force availability, assumptions established earlier, and coordination/deconfliction). Availability analysis must extend to support and synchronization issues for each capability. For instance, when use of particular capabilities will require intelligence support for BDA, such support must be coordinated through J-2. When capabilities may be assigned to other tasks, selection for IO tasking must be coordinated among staff functions, components, or supporting organizations as appropriate.

c. Assign specific tasks to selected capabilities to achieve ~~prioritized~~ sub-objectives. Coordinate and deconflict level of effort required of each capability for each task if not specified when determining availability.

d. Finalize the IO synchronization matrix and provide to the JPG for inclusion in the synchronization matrix of the entire operation.

~~*See paragraphs and above for discussion of integration, synchronization and coordination/deconfliction. See paragraphs below for discussion of the elements of " The Art of Information Operations." See Appendix G, "Current Information Operations Planning Methodologies, Support Systems, and Tools," for discussion of strategy to task methodology. See paragraph below for discussion of development of IO tasks. See Tab 6, "Concept Development Combatant Commander's Concept," to Annex B, "Deliberate Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," provides more detailed discussion about IO planning tasks in this step of the deliberate planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

(6) **Chairman of the Joint Chiefs of Staff Estimate.**

(a) The purpose of this step is to formally examine the combatant commander's concept in accordance with policy established in CJCSI 3141.01 Series, *Responsibilities for the Management and Review of* ~~*OPLANS*~~ *Operation Plans*, and procedures established in CJCSM 3141.01 Series, *Procedures for the Review of Operation Plans*. CDRUSSTRATCOM also reviews the IO portions of the concept in this step for coordination of IO across ~~geographic AOR~~ combatant command boundaries.

(b) Key IO staff actions related to the Chairman of the Joint Chiefs of Staff Estimate include:

1. **Research and answer questions** posed by CJCS during review.

2. **Coordinate and deconflict the revision of the concept** as required to complete the CJCS review.

~~*See Tab 7, "Concept Development – Chairman of the Joint Chiefs of Staff Estimate," to Annex B, "Deliberate Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this step of the deliberate planning process in JOPES. See also Appendix A, "Supplemental Guidance," (published separately).*~~

c. **Phase III Plan Development.**

(1) During this phase the IO staff develops the IO details of the ~~of~~ plan.~~:~~

(2) Key IO staff actions during plan development include:

(a) Coordinate and deconflict through the IO cell and participate in other planning meetings and processes to **support specific steps** in the plan development phase.~~:~~

~~1. Force planning.~~

~~2. Support planning.~~

~~3. Chemical/nuclear planning.~~

~~4. Transportation planning.~~

~~5. Noncombatant evacuation operations (NEO) planning.~~

~~6. Shortfall identification.~~

~~7. Transportation feasibility analysis.~~

~~8. TPFDD refinement.~~

~~9. Documentation.~~

(b) **Develop core capability synchronization matrices** to support the IO synchronization matrix. Coordinate and deconflict supporting and related capability matrices developed by appropriate staff sections.

(c) **Supplement automated planning tools** ~~discussed in Appendix G, "Current Information Operations Planning Methodologies, Support Systems, and Tools,"~~ **with local forms** to organize detailed information for planning purposes.

(d) **Participate in TPFDD refinement** to ensure the necessary IO forces are appropriately placed in the flow of forces into the ~~AOR~~ operational area.

(e) **Draft designated portions of the planning document.** ~~In deliberate planning the IO staff is normally responsible for portions of the planning document shown in Annex D, "Location of Information Operations Guidance in JOPES Formats," to Appendix C, "Information Operations in JOPES Planning Processes."~~

~~*See Tab 8, "Plan Development Phase," to Annex B, "Deliberate Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this phase of the deliberate planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

d. **Phase IV Plan Review.**

(1) The purpose of this ~~step~~ phase is to formally examine the combatant commanders plan in accordance with policy established in CJCSI 3141.01A, *Responsibilities for the Management and Review of ~~OPLANS~~ Operation Plans*, and procedures established in CJCSM 3141.01A, *Procedures for the Review of Operation Plans*. CDRUSSTRATCOM also reviews the IO portions of the plan in this step for coordination of IO across ~~geographic AOR~~ combatant command boundaries.

(2) Key IO staff actions during plan review phase include:

(a) **Research and answer questions** posed by CJCS during review.

(b) **Coordinate and deconflict revision of plan** as required to complete CJCS review.

~~*See Tab 9, "Plan Review Phase," to Annex B, "Deliberate Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this phase of the deliberate planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

e. **Phase V Supporting Plans.**

(1) Supporting plans are normally developed by supporting combatant commands, components, and the DOD ~~components~~ combat support agencies tasked to support the plan. Normally, these organizations will conduct parallel planning while the supported combatant commander's staff is developing the deliberate planning product. Development of supporting plans is usually well underway by the time the Chairman of the Joint Chiefs of Staff approves a deliberate planning product. Timelines for development and submission of supporting plans are

established in CJCSI 3141.01 Series, *Responsibilities for the Management and Review of ~~OPLANS~~ Operation Plans*, and procedures established in CJCSM 3141.01 Series, *Procedures for the Review of Operation Plans*. The supported combatant commander approves supporting plans. Supporting plans focus on mobilization, deployment, employment, sustainment, and redeployment.

(2) Key supported combatant commander's IO staff actions during supporting plan development include:

(a) **Keep organizations responsible for development of supporting plans informed of details of plan development (as access restrictions allow)** throughout the deliberate planning process to facilitate development of supporting plans.

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

~~*See Tab 10, "Supporting Plans," to Annex B, "Deliberate Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this phase of the deliberate planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

10. Crisis Action Planning

The complexity and long term nature of ~~many~~ IO information ~~and~~ requirements ~~information dimension "shaping" actions~~ do not give ~~IO~~ planners all the capability options that might be available in deliberate planning. Ideally, crisis action planning can build on an existing OPLAN or longer term themes and action already underway in the AOR through execution of a TSCP. However, IO planners must be prepared to adapt to unforeseen situations and develop the IO portion of a crisis action planning product that matches the scope and timeline of an emerging crisis with available forces and plans for the employment of those forces with TTP limited to those that can be reasonably expected to be effective within the constraints imposed by the situation or other considerations. Each command modifies the JOPES crisis action planning process as needed. In contrast to deliberate planning, crisis action planning normally takes place in a compressed time period. Coordination and deconfliction between IO capability, staff functions, and various organization ~~is~~ are even more crucial than in deliberate planning. Discussion here is focused on how an IO staff at the **combatant command level** might participate in crisis action planning processes. IO specific staff actions during crisis action planning through Phase IV, Course of Action Selection~~,~~ are the same as during deliberate planning. Discussion of crisis action planning phases will reference actions described previously in deliberate planning. Staff actions mentioned are nominal and should be modified and adapted as each planning project requires. If a JTF staff with appropriate IO staff is responsible for crisis action planning, the assumption is made that either a ~~SJTF~~ SJFHQ or a core of experienced JTF-level planners provided by USJFCOM, will organize and direct the planning effort. ~~The section on JTF IO staff organization in Chapter VI, "Responsibilities and Command Relationships," makes reference to the SJTF SOP. If that document is being used as the basis for JTF procedures and organization, recommended actions in this section should be modified to~~

~~accommodate local staff procedures and organization.~~ Figure V-3, provides a general guide to IO planning as an integrated part of crisis action planning at the combatant command level. Planning tasks in Figure V-3 may be adapted for crisis action planning at the ~~,~~**subordinate joint command level, JTF level** or the **component level**, as required.

a. **Phase I Situation Development.**

(1) Situation development may take place over a period of days, months or even years. During this phase, intelligence personnel monitor the situation in the ~~CC's~~ AOR, with a focus on the combatant commander's PIRs and watch for any developments with the potential to

INFORMATION OPERATIONS PLANNING RELATED TO CRISIS ACTION PLANNING

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

CJCS Chairman of the Joint Chiefs of Staff
IO Information Operations
JOPES Joint Operation Planning and Execution System
TPFDD Time-Phased Force and Deployment Data

Figure V-3. Information Operations Planning Related to Crisis Action Planning

destabilize the AOR. If any of the developments in the AOR convince the ~~CC~~ JFC that there is a potential crisis developing, the ~~CC~~ JFC may issue an operation report-3 ~~report to~~ through the Chairman of the Joint Chiefs of Staff to the Secretary of Defense (SecDef), stating his assessment of the situation. At this stage, it's time for the IO ~~C~~cell to begin monitoring the situation, identifying intelligence gaps necessary for IO and formulating RFIs to be submitted to the J-2.

(2) Key IO staff actions during situation development include:

(a) As the crisis develops, the IO cell should convene on a regular basis to review the situation and determine what preliminary planning actions should be accomplished to prepare for crisis action planning. The challenge is normally to balance tasking intelligence and supporting organizations in anticipation of a crisis against competing demands from other staff sections, other commands, and perhaps ~~AOR's~~ AORs.

(b) Begin taking actions discussed in the Initiation Phase of the deliberate planning.

~~*See Tab 1, "Situation Development Phase," to Annex C "Crisis Action Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this phase of the crisis planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

b. **Phase II Crisis Assessment.** During this initial assessment the IO staff derives guidance from two sources: the commander's initial guidance and the higher headquarters' OPLAN/OPORD.

(1) After reviewing the combatant commander's assessment, the SecDef will either direct the combatant commander to continue monitoring or ~~they~~ he will issue a warning order through the Chairman of the Joint Chiefs of Staff, directing the combatant commander to begin planning. The warning order may prescribe one or more COAs to be considered and will apportion forces to the combatant commander for planning purposes. Upon receipt of the ~~W~~warning ~~O~~order, formal planning begins on an accelerated timeline. The time available for planning may be specified in the ~~W~~warning ~~O~~order or be established by the combatant commander.

(2) Key IO staff actions during crisis assessment include:

(a) **Assign and coordinate tasks from ~~I~~initiation ~~P~~phase and the ~~M~~mission ~~A~~analysis and ~~P~~planning ~~G~~guidance steps of the ~~C~~concept ~~D~~development ~~P~~phase of deliberate planning.**

(b) **Evaluate the need ~~of~~ for additional planning augmentation or collaborative support** above what might be required for deliberate planning. ~~Taylor~~ Tailor the quantity and skill sets in augmentation requests to the specifics of mission and concept of operations ~~is~~ as they are developed.

~~*See Tab 2, "Crisis Assessment Phase," to Annex C "Crisis Action Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this phase of the crisis planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

c. **Course of Action Development.**

(1) During ~~course of action~~ COA development, the IO staff supports the development of ~~courses of action~~ COAs as specified in the commander's guidance. Unlike deliberate planning, however, the combatant commander does not select the COA in crisis action planning. Instead, a ~~C~~commander's ~~E~~estimate, describing each ~~course of action~~ COA and recommending a specific ~~course of action~~ COA is submitted to ~~the SECDEF~~ SecDef through the Joint Staff. ~~The Secretary of Defense~~ SecDef will select the ~~course of action~~ COA.

(2) Key IO staff actions during ~~course of action~~ COA development include assignment and coordination of tasks from the ~~S~~staff ~~E~~estimates and ~~C~~commander's ~~E~~estimate steps of the Concept Development Phase of deliberate planning for all of the ~~courses of actions~~ COAs to be presented to ~~the Secretary of Defense~~ SecDef in the crisis action ~~C~~commander's ~~E~~estimate. Accelerated development of staff estimates may require modification of normal staffing processes and closer coordination between members of the IO cell.

~~*See Tab 3, "Crisis Action Development Phase," to Annex C "Crisis Action Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this phase of the crisis planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

d. **Course of Action Selection.**

(1) The SecDef will select the COA and direct the combatant commander to proceed according to various timelines. On slower timelines, the combatant commander is directed to continue planning and monitoring the situation for an indeterminate or specified period or until specific events occur. More ambitious timelines may include the issuance of an alert order, ordering supported and supporting commands and supporting DOD organizations to begin preparing to execute the mission. In an acute crisis, ~~the Secretary of Defense~~ the situation may require an immediate execution order.

~~(2) Regardless of the timeline, as soon as a course of action is selected, the IO cell commences developing a complete IO plan as described in the deliberate planning process, developing synchronization matrices, IO planning worksheets, and execution checklists. Even when a slower planning timeline has been selected the dynamics of the emerging crisis may cause subsequent acceleration of the planning process.~~

(2) Key IO staff actions during COA selection include assignment and coordination of tasks from the Chairman of the Joint Chiefs of Staff ~~R~~review step of the ~~C~~concept

~~D~~development ~~P~~phase of deliberate planning. ~~Normal staff planning processes and level of coordination are modified to meet the specified timeline.~~

~~*See Tab 4 "Course of Action Selection Phase," to Annex C "Crisis Action Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this phase of the crisis planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

e. **Execution Planning.**

(1) Regardless of the timeline, as soon as a COA is selected, the IO cell commences developing a complete IO plan as described in the deliberate planning process, developing synchronization matrices, IO planning worksheets, and execution checklists. Even when a slower planning timeline has been selected the dynamics of the emerging crisis may cause subsequent acceleration of the planning process. During crisis action planning, current events and intelligence and other information details are available and must be incorporated in the plan as it is developed. ~~Supporting plans, subordinate joint commander planning, and component planning must occur during execution planning, often simultaneous. Simultaneous planning at multiple levels complicates integration and synchronization and may require addition coordination procedures to be established. Local SOP's may anticipate the requirement for multi-level simultaneous planning and specific additional coordination procedures to be implemented.~~

(2) Key IO staff actions during ~~course of action~~ COA selection include assignment and coordination of tasks from the ~~P~~plan ~~D~~development ~~P~~phase of deliberate planning, ~~and~~ refined with details normally not available ~~in~~ during deliberate planning. ~~Normal staff planning processes and level of coordination are modified to meet the specified timeline.~~

~~*See Tab 5 "Execution Planning Phase," to Annex C "Crisis Action Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning Processes," for more detailed discussion about IO in this phase of the crisis planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

f. **Execution.**

(1) The execution phase of crisis action planning involves ~~the conversion of~~ converting the completed plan into an OPORD~~ER~~ and then assisting the commander in directing the execution of the plan. Actions specified for the execution phase below occur at both ~~at both~~ the combatant command and subordinate joint command levels and are modified accordingly.

(2) Key IO staff actions during the execution phase include:

(a) Draft IO portions of the OPORD as directed by the J-3.

(b) Develop execution worksheets or checklists for each core, supporting and related capability to be executed in the plan based on capability planning worksheets described during plan development in deliberate planning. The core capability staff sections within the

joint IO cell develop their respective execution worksheets coordinating with other IO capability staff sections, other command levels, and among supporting organizations and multinational forces as appropriate. Close and continuous coordination with Service and functional component staffs is essential to development of execution worksheets. Staff sections responsible for supporting and related IO capabilities at each level of joint command develop their own worksheets. The IO officer should obtain copies of all supporting and related capability execution worksheets and direct their compilation into a master execution matrix or worksheet for ~~easy~~ ease of cross reference.

(c) The IO staff, under the direction of the IO officer, should develop a daily execution worksheet. Daily worksheets are used to correlate daily capability activities with operational and intelligence feedback. ~~The format of the daily worksheet should be specified in local SOPs.~~ The daily worksheet should be developed using database or spreadsheet software that is, at a minimum, standardized across the entire staff at each level of command. Staff specific IM procedures, specified in local instructions or SOPs, may direct the use of specific software for operational coordination purposes.

(3) At some point in the execution phase, joint staff manning and procedures normally shift to some local version of "execution mode." The JOC may already have transitioned to a higher state of readiness as a crisis develops. The IO staff should plan for requirements to man specific IO watch positions in the JOC and in core capability staff sections during longer hours as the execution phase nears. Depending on the role of IO in the early phases of an operation, the IO staff may have to shift to "execution mode" prior to the remainder of the staff. Once the staff battle rhythm of execution becomes "routine" during the execution phase, manning and staff procedures may shift again ~~to again~~ to accommodate long term sustainment of "execution mode." At the other end of an operation, during a transition back to peace or the normalization of staff activity, the IO staff may be required to continue at a heightened state of readiness to supervise extensive IO in support and stabilization operations.

(4) Once the IO staff has transitioned to a heightened state of staffing to monitor execution, key IO staff actions should include:

(a) Man designated JOC and core capability staff sections as specified in local SOPs.

(b) Conduct IO cell meetings at a frequency established in local SOPs in coordination with the local staff battle rhythm and cyclical operations deadlines (e.g., development of the ATO). Local IO-specific instructions or SOPs should establish a routine for conduct of IO cell meetings (during both routine meetings and execution phase meetings).

(c) Establish coordination and support procedures among various levels of command and among supporting organizations and multinational forces.

~~*See Tab 6 "Execution Phase," to Annex C "Crisis Action Planning Process," of Appendix E, "Information Operations in Joint Operations Planning and Execution System Planning*~~

~~*Processes," for more detailed discussion about IO in this phase of the crisis planning process. See also Appendix A, "Supplemental Guidance," (published separately).*~~

11. Joint ~~IO~~ Information Operations Planning Process

The JIOPP provides a logical, structured method for integrating IO planning into the JOPES deliberate and crisis action planning processes. The JIOPP is subdivided into the Joint IO Attack Planning Process (JIOAPP) and the Joint IO Defensive Planning Process. (JIODPP).

a. **JIOAPP.** The JIOAPP facilitates offensive IO planning at the combatant command and subordinate joint and/or component commands and the integration of offensive IO tasks with defensive IO tasks as well as other operational tasks. Combatant command IO planning usually has as its objective the construction of detailed IO task statements that are provided to the ~~C~~components for further planning. Component-level planning strives to determine the optimum match between the combatant commander objectives and targets, as well as IO means (weapons) and targets. The JIOAPP is highly collaborative in nature. Information and expertise from sources and staffs outside the IO cell are normally needed to apply the JIOAPP most effectively. ~~Annex A to Appendix F provides detailed step-by-step guidance on the JIOAPP.~~

b. **JIODPP.** The JIODPP facilitates defensive IO planning at the combatant command and subordinate joint and/or component commands and the integration of defensive IO tasks with offensive IO tasks as well as other operational tasks. ~~Annex B to Appendix F provides detailed step-by-step guidance on the JIODPP.~~

SECTION C. ~~SUBJECTIVE~~ SITUATIONAL ASPECTS OF INFORMATION OPERATIONS PLANNING

12. General

IO cannot be planned with a ~~"cookie cutter"~~ universal approach. IO planning requires a synthesis of TTP with consideration given to situational variations in the operational environment. The dynamic nature of the information ~~dimension~~ environment, discussed in Chapter I, "Introduction," makes each planning project unique. Good IO planning depends on planners trained and educated as discussed in Chapter VII, "Information Operations in Joint ~~Training,~~ Education, Training, Exercises, and ~~Experimentation~~ Experiments," working as a team across organizational and functional boundaries. Many aspects of IO planning, like joint planning, are subjective. This section relates the elements of operational art from JP 3-0, *Joint Doctrine for Operations*, to IO planning, discusses the commander's intent and/or guidance in relation to IO planning, and the development of IO objectives, tasks, and concepts of operation as part of the overall planning effort.

13. The Art of Information Operations

a. Operational art is the use of military forces to achieve strategic goals through the design, organization, integration, and conduct of strategies, campaigns, major operations, and battles.

~~JFCs employ operational art, in concert with strategic guidance and direction received from superior leaders, in developing campaigns and operations. **JFCs employ air, land, sea, space, and special operations forces in a wide variety of operations in war as well as in support and stability operations**.~~ Joint operational art looks not only at the employment of military forces but also at the arrangement of their efforts in time, space, and purpose. Joint operational art, in particular, focuses on the fundamental methods and issues associated with the synchronization of air, land, sea, space, and special operations forces. Strategies, campaigns, operations, and battles occur in both ~~a~~ the physical ~~dimensions~~ domains (land, sea, air, or space) and the information ~~dimension~~ environment simultaneously. **Offensive IO tasks may be assigned to air, land, sea, space, and special operations forces. Likewise, all these forces must be protected by defensive IO actions**.

~~b. **IO art focuses on the fundamental methods and issues associated with synchronization of military effort in the information dimension.** Successful IO art completely integrates with the synchronization of military forces in the physical dimension. Like operational art, the art of IO requires broad vision, the ability to anticipate, and effective joint, interagency, and multinational cooperation. Well-trained, experienced IO planners contribute seamlessly to the broader operational artistry of the joint planning effort. Among many considerations, IO art requires planners to answer the following questions:~~

~~(1) What information conditions must be produced in the operational area to achieve the joint force commander's (JFC) goal? (Ends)~~

~~(2) What sequence of IO actions is most likely to produce that condition? (Ways)~~

~~(3) How should the IO resources of the joint force be applied to accomplish that sequence of actions? (Means)~~

~~(4) What is the likely risk to the joint force, civil populace, or unintended "targets" in performing that sequence of IO actions? (Risk assessment)~~

~~e~~b. ~~To the degree that military objectives, at any level, are achievable through the information dimension, IO is useful to achieve those objectives.~~ IO are useful, at any level, when objectives are achievable through the information environment. **When the information ~~dimension~~ environment is a primary dimension to achieve military objectives, IO may be a primary means.** ~~When~~ DOD missions require ~~that~~ IO when joint forces lead or support a wider USG or allied/coalition effort~~s~~ in the information ~~dimension, wholly or partially, IO may be used~~environment. IO must always be planned and executed in concert with other USG and/or allied/coalition informational activities and/or conventional military operations, after the moral, ethical, legal, and potentially disruptive issues with regard to civilian information usage, are considered. These issues, and how to account for them, are discussed in later chapters.

c. **The same fundamental elements that characterize operational art as a whole characterize the art of IO.** These elements~~, as discussed in Chapter III of JP 3-0,~~ are expanded on below to relate IO to their overall operational purpose. The relationship of IO ~~IO's relationship~~ to the various operational art elements is only introduced here.

(1) **Synergy** is a concept that relates to integrating and synchronizing operations. In combat operations, JFCs not only attack the adversary's physical capabilities, but also the adversary's morale and will. JFCs integrate and synchronize operations in a manner that applies force from different dimensions to shock, disrupt, and defeat opponents. In combat operations, IO may be used to apply force psychologically, electronically, and/or physically ~~in the information dimension, in concert with the other elements of combat power, to attack physical capabilities and the adversary's morale and will~~. It is difficult to view the contributions of air, land, sea, space, special operations forces and IO in isolation. Each may be critical to the success of the joint force, and each has certain unique capabilities that cannot be duplicated by other types of forces. Given the appropriate circumstances, any dimension of combat power can be dominant — and even decisive — in certain aspects of an operation or phase of a campaign, and each force can support or be supported by other forces. The JFCs are especially suited to develop and project joint synergy given the multiple unique and complementary capabilities available only within joint forces. ~~Likewise, in~~ In concert with the other elements of combat power, IO ~~is~~ are useful in defending friendly capabilities, morale and will and attacking those of an adversary. Synergy is a primary goal of the planned integration of various IO capabilities to achieve specific military objectives.

(2) **Simultaneity and ~~d~~Depth.** ~~are used to bring force to bear on the opponent's entire structure in a near simultaneous manner.~~ In combat operations, IO that complement the simultaneity and depth of the physical attack in the information ~~dimension~~ environment may contribute to the adversary's collapse. ~~Simultaneity also refers to the concurrent conduct of operations at the tactical, operational, strategic, and national levels. Since the information dimension is ubiquitous across the globe,~~ IO simultaneity in multiple theaters is necessary. ~~Multi-theater~~ Multitheater IO reinforces theater-specific IO and counters unintended consequences that may result from IO actions executed for specific theaters. ~~Defensively,~~ IO can help to disrupt adversary simultaneity and depth.

(3) **Anticipation.** ~~is the key to effective planning so as to remain alert for the unexpected and for opportunities to exploit the situation.~~ Situational awareness is a prerequisite for commanders and planners to be able to anticipate opportunities and challenges. Defensive IO helps to preserve the quality of the JFCs situational awareness. Offensive IO degrades the adversary's situational awareness. It should be noted, however, that anticipation is not without risk. Commanders and planners that tend to lean in anticipation of what they expect to encounter are more susceptible to operational ~~military deception (~~MILDEC~~)~~ efforts by an opponent. Defensive IO helps to guard against this susceptibility. IO exploits anticipation by the adversary through MILDEC and other capabilities.

(4) **Balance** is ~~an appropriate mix of forces and capabilities within the joint force~~the maintenance of the force, its capabilities, and its operations in such a manner as to contribute to freedom of action and responsiveness. In each strategy, campaign, operation, and battle there is a balance between IO and other types of effort. JFCs designate priority efforts and establish appropriate command relationships to assist in maintaining the balance of the force. Military deception and offensive information operations, direct attack of adversary strategic centers of gravity (COGs), interdiction, and maneuver all converge to confuse, demoralize, and destroy the

opponent. Each application of IO involves an internal balance of differing capabilities to most efficiently complement other efforts and achieve assigned objectives. The risk management functions of IO, particularly in defensive IO, reflect a balance between level of risk and resources applied to counter that risk.

(5) **Leverage.** ~~is used to impose a force's will on the adversary, increase the adversary's dilemma, and maintain the initiative.~~ JFCs arrange symmetrical and asymmetrical actions to take advantage of friendly strengths and adversary vulnerabilities and to preserve freedom of action for future operations. ~~JFCs must take action to protect or shield all elements of the joint force from adversary symmetrical and asymmetrical action.~~ IO contributes to friendly information superiority by exploiting, disrupting and denying adversary use of the information ~~dimension~~ environment while helping to protect against adversary ~~attempts to use symmetrical and asymmetrical~~ information attacks against friendly forces and societies.

(6) **Timing and ~~t~~Tempo.** ~~serve to assist forces in dominating the action, remaining unpredictable, and operating beyond the adversary's ability to react, with the goal being to exploit friendly capabilities and inhibit the adversary.~~ JFCs plan and conduct operations in a manner that synchronizes the effects of operations so that the opponent feels the maximum force of their contributions at the desired time. ~~IO is applicable as a primary or support effort across the spectrum of conflict from peace, through crisis and war, and back to peace.~~ Some level of IO effort is appropriate on a continuing basis during peacetime to promote strategic goals. During peacetime, DOD IO complements and supports other USG efforts. During periods of crisis, the tempo of IO increases to deter the outbreak of hostilities or, failing to deter, to favorably shape the information ~~dimension~~ environment in preparation for the outbreak of hostilities. During hostilities, IO timing and tempo synchronize with other elements of combat power. Adjustments are made to the timing and tempo of various capabilities, within the IO effort itself, to best enhance the other characteristics of operational art. Following the conclusion of hostilities, IO ~~is~~ are paced to help stabilize the situation to friendly advantage and facilitate the achievement of strategic goals.

(7) **Operational ~~r~~Reach and ~~a~~Approach.** ~~is about the range in which the joint force can prudently operate or maintain effective operations, emphasizing that basing, in the broadest sense, is an indispensable foundation of joint operational art.~~ IO extends the operational reach and approach of the JFC. The global nature of the information ~~dimension~~ environment enables the commander to employ IO from any geographic position without regard for physically proximity to the AOR. ~~At the same time,~~ Global communications and information infrastructure require that friendly forces, infrastructure, and citizens ~~must~~ be protected from information attack and exploitation regardless of their physical proximity to the adversary.

(8) **Forces and functions** of the adversary are typically targeted by joint force operations concurrently, in order to create the greatest possible contact area between friendly and adversary forces. The need for information by all forces and functions creates opportunities to use IO against both forces and functions. Use of IO to attack C2, logistics, or intelligence functions may lead to confusion, uncertainty, or lack of confidence in information systems and may contribute directly to collapse of adversary capability and will. The nonlethal nature of many IO capabilities allows their use prior to and after hostilities, extending contact across time

as well as space and thereby giving the friendly force greater opportunity to influence events and outcomes favorably.

(9) **Arranging operations** will often consist of a combination of simultaneous and sequential operations to achieve the desired end state conditions quickly and at the least cost in personnel and other resources. IO are arranged with other DOD efforts and with other USG or allied/coalition efforts. Internal to IO, specific capabilities are arranged to achieve the desired objective efficiently consistent with the other elements of operational art.

(10) ~~**Centers of gravity (**~~**COGs**~~**)**~~ are those characteristics, capabilities, or locations from which a military force derives its freedom of action, physical strength, or will to fight. Identification of adversary COGs requires detailed knowledge and understanding of how opponents organize, fight, and make decisions, as well as their physical and psychological strengths and weaknesses. Different types of COGs will have different reliance on information that creates vulnerabilities that can be attacked or exploited with IO capabilities. The vulnerabilities of friendly COGs to information attack must be understood so that appropriate measures, including defensive IO, can be planned and implemented.

(11) **Direct versus ~~I~~indirect** refers to the JFC's attacking of adversary COGs directly or indirectly. Where direct attack means attacking into an opponent's strength, JFCs should seek an indirect approach. The JFC determines whether IO ~~is~~ are a planned part of the direct approach, indirect approach, or a combination of both. Considering the core capabilities of IO, analysis should include evaluation of TTP to refine or create indirect attacks of adversary COGs. Considerations for making this decision include the type of mission assigned to the joint force and the adversary's information strengths and weaknesses.

(12) **Decisive points** can assist a force in gaining a marked advantage over the adversary and may greatly influence the outcome of an action. Decisive points are key to attacking COGs. Decisive points in the information ~~dimension~~ environment can be geographic, psychological, or electronic. Critical points where information is stored or processed, or through which information is routed in communications, are examples of decisive geographic points. Adversary leader's or ~~soldiers~~ military personnel knowledge of the loss of key military defensive positions are examples of a psychological decisive points. Critical information requirements, information processing or storage capability, or uses of the electromagnetic spectrum for C2 are examples of decisive electronic points. There will normally be more decisive points in an operational area than JFCs can control, destroy, or neutralize with available resources. The commander designates the most important decisive points as objectives and allocates resources to control, destroy, or neutralize them. IO extends a commander's resources to achieve objectives by allowing some points to be controlled, destroyed or neutralized through ~~nonlethal~~ non-kinetic means. The ~~nonlethal~~ non-kinetic and covert aspects of some IO capabilities give commanders options to control, destroy, or neutralize~~d~~ objectives prior to the outbreak of hostilities if proper authority has approved such actions.

(13) **Culmination** has both an offensive and defensive application in combat operations. In the offense, the culminating point is the point in time and space at which an attacker's combat power no longer exceeds that of the defender. Success in the attack at all

levels is to secure the objective before reaching culmination. ~~Offensive IO supports this goal in combat operations.~~ A defender reaches culmination when the defending force no longer has the capability to go on the counteroffensive or defend successfully. IO may directly seek~~s~~ early culmination of adversary capabilities and delayed culmination of friendly capabilities. Additionally, IO may influence the conflict by deception. Causing an adversary to cease resistance prematurely, forego a viable counteroffensive, attack with insufficient force, or cease an attack prematurely are examples of effective IO.

(14) **Termination** is an essential component of strategy and operational art, whereby forces know when to terminate military operations and how to preserve achieved advantages. A period of post conflict activities exists from the immediate end of the conflict to the redeployment of the last United States Service member. Also, a variety of operations other than war occur during this period to ensure political objectives are achieved and sustained. IO ~~is~~ are an important aspect of post conflict operations. The end of combat operations only marks the transition of IO efforts from one phase to another. Even after the redeployment of all United States forces, IO normally continue remotely in concert with other USG efforts to ensure maintenance of achieved gains and promote long-term United States strategic goals.

14. Commander's Intent and Information Operations

a. Commanders should provide as much specific guidance on IO as possible in order to ensure the development of a clear concept of support with specific objectives, tasks, and MOEs. ~~Vague statements about IO such as "I need robust and proactive full spectrum IO to establish and maintain information dominance throughout the JOA" are insufficient to plan IO in the detail required in JOPES planning products.~~

b. The commander's vision of IO's role in an operation should start with initial guidance. ~~The commander's initial guidance normally emerges from an exchange of information between the commander and his staff..~~ 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 exchange of information about IO ~~is~~ are appropriate. For example, separate guidance on IO may be appropriate during peace operations or other missions where information may be the principal or only means that the commander has available to ~~generate combat power~~influence an adversary. Separate, detailed guidance may also be appropriate in situations where a commander or staff is inexperienced in IO. 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 concept during actual operations.

c. IO-related topics that may be addressed in commander's intent or guidance include:

(1) When IO ~~is~~ are in a supporting role in plan or operation and when it is the supported effort.

(2) Specific reference to strategic communications themes and messages that ~~AOR~~ IO should be focused on or deconflicted.

(3) Level of effort in relation to other operational efforts broken down by operational phase.

(4) Cultural or political sensitivities or concerns of adversaries, allies, and neutral nations within the ~~AOR~~ operational area which IO in the current plan or operation must be sensitive to or avoid.

SECTION D. INFORMATION OPERATIONS MEASURES OF PERFORMANCE AND EFFECTIVENESS

~~15. Criteria of Information Operations Measures of Effectiveness~~

~~MOE for IO present some unique challenges. IO planners or exercise developers should work with intelligence or training personnel, and other expertise, when available, to ensure that the following criteria are consider in development of IO MOE:~~

~~a. **Appropriate.** IO MOE should correlate to appropriate purposes they support. Training MOE should be selected to gage the effectiveness of IO in achieving specific training objectives. Operational MOE should assist in providing operational feedback required to adjust plans as operational are executed. Over longer periods of time MOE can contribute to research, development, and lessons learned development. IO MOE should also be appropriate to the level of command requiring feedback. The same operation may have different MOE for strategic, operational, and tactical purposes.~~

~~b. **Mission-related.** MOE should correlate to the overall mission and its objectives.~~

~~c. **Task-related.** Where possible tie specific MOE to specific IO tasks to gage the relative effectiveness of specific IO TTP.~~

~~d. **Measurable.** Quantitative MOE are the measure of choice when the situation permits their use. Physical and electronic indications of change in the information dimension are more easily quantified than psychological changes. When non-quantitative MOE, interpretation of feedback information should be conducted, when possible, by personnel or methods that remove subjective bias from the results.~~

~~e. **Comparable.** Ideally, IO MOE are comparable across AOR boundaries and time by mission type. MOE that are comparable can be analyzed over time for research, development, and lessons learned purposes.~~

~~f. **Resource efficient.** The requirements to collect training, intelligence, or open source information to calculate IO MOE should be appropriate to the personnel, budgetary, and material resources available to apply to such requirements when prioritized against competing requirements.~~

~~g. **Timely.** Operational MOE should be appropriate to the time frame of feedback required. IO plans that are dependent on MOE feedback requiring lengthy intelligence collection and analysis processes are not realistic.~~

~~**16. Development of Information Operations Measures of Effectiveness**~~

~~MOE only are limited by the imagination of commanders and their staffs. However, they should exercise a certain degree of caution and judgment when using statistical indicators alone. These indicators may vary widely in interpretation, may be valid only for a specific time, place, or group of people, and may not have a direct correlation to effectiveness.~~

~~*See CJCSM 3500.04,* Universal Joint Task List (UJTL)*, and CJCSM 3500.04,* Classified Supplement To The Universal Joint Task List (UJTL)*, for information about MOE for IO tasks joint forces are. expected to be capable of accomplishing.*~~

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

Performance of IO activities is measured in order to gauge the commitment levels of the various IO capabilities and **mission performance**. This allows decisions to be made on the correct level of IO resources to apply to a particular operation. **Effectiveness** of IO activities is measured in order to determine whether the activities being conducted are having the desired effect and to what extent this is happening i.e., **mission accomplishment**. This allows decisions to be made on the achievement of IO objectives and therefore the continuation, amendment, or cessation of specific activities. The relationship between these two measures is illustrated in Figure V-4.

THE RELATIONSHIP BETWEEN MEASURES OF PERFORMANCE AND MEASURES OF EFFECTIVENESS

Capability	Measures of Performance (MOP)*	Measures of Effectiveness (MOE)**	Remarks
Psychological Operations (PSYOP)	Impact of the effects of weather on dissemination of PSYOP products	Effect of PSYOP messages on actions or perceptions of specified audiences	MOE requires access to the target audience
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)	Identify possible OPSEC measures and select specific measures for execution	Evidence of adversary decisions made based on collected information	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	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 electronic attacks conducted	Effect of electronic attack on target systems	MOE requires access to a measurable output or to the adversary's own reporting of the attack
Public Affairs (PA)	Instances of errors in released information Percentage of requests for information answered	Effect of errors on target audience perceptions Effect of media releases on perceptions of specific target audiences	MOE are answered by targeted and responsive media monitoring and attitude surveys
Civil Affairs (CA)	Weeks to identify Host Nation Support (HNS) contractor resources	Attitude of HNS contractors to US/ally forces	MOE requires an attitude survey of contractors

*MOP are taken from UJTL IO Tasks Information Operations Tasks Extracted From CJCSM 3500.04C, Universal Joint Task List (UJTL) 1 July 2002c. Most MOP are answered by internal statistic generation.

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

Figure V-4. The Relationship Between Measures of Performance and Measures of Effectiveness

16. General Criteria for Information Operations Measures of Effectiveness

Without a clear statement of the objective or task, it is impossible to measure progress towards it. It follows, therefore that IO staffs must consider both the objective and its related MOEs as one during planning. In developing IO MOEs, the following general criteria should be considered:

a. **Objective/Task Related.** MOEs should directly relate to either the overall IO objectives, sub-objectives, or specific related tasks.

b. **Measurable.** MOEs must actually be measurable, and preferably quantitatively (i.e., expressed numerically relative to a previous baseline figure). Where qualitative MOEs are used, interpretation of feedback information should be conducted, when possible, by personnel or methods that remove subjective bias from the results. The use of appropriately qualified and experienced analytical staff will be important in ensuring that both statistical and qualitative judgments are credible. MOEs should only be developed if the necessary capability to gather data is available.

c. **Timely.** Some IO objectives and tasks will require feedback from MOEs in a short timeframe; others will be susceptible to longer-term measurement. The required feedback time should be clearly stated for each MOEs and a plan made to report against that timeframe.

d. **Properly Resourced.** The collection, collation, analysis and reporting of MOEs data requires personnel, budgetary, and material resources. IO staffs should ensure that these resources are built into the IO plan as objectives and tasks are developed.

17. Development of Information Operations Measures of Effectiveness

IO MOEs will be developed throughout the JOPES process so that the final plan, with its associated IO annex, is supported by robust, relevant and useful MOEs. The stages in the process and related MOEs development activity are:

a. **Mission Analysis.** The IO product from mission analysis becomes the draft IO objectives. These should be supported by proposed MOEs. At this stage, MOEs will be general and may not be susceptible to measurement as a single entity - they would likely require several individual measures to gauge overall success.

b. **Commander's Planning Guidance.** The Commander's Planning Guidance will normally direct a number of COAs to be developed. The IO staff will examine each COA for any particular IO objectives and tasks and ensure that these are included in the planning order. Possible MOEs related to specific IO objectives and tasks will be noted for further development.

c. **Staff Estimates.** During the IO staff estimate specific draft IO objectives and tasks will be developed for each COA. Specific MOEs are developed for each draft objective and task at this stage and the resource implications are noted.

d. **Commander's Estimates and Confirmed Concept.** During the commander's estimate, a specific COA is chosen. From this, the IO objectives, tasks and MOEs are confirmed and the resource requirements for all aspects of IO, including MOEs, become clear.

e. **Plan Development.** During plan development, the IO staff establish the requirements for conduct of IO and MOEs in the plan. Responsibilities for collection, collation, analysis and reporting for each MOEs are laid down in the plan or by subsequent fragmentary order.

18. Examples of Information Operations Measures of Effectiveness

a. Quantitative MOEs

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

(2) Number of civil disturbances over time as reported by own forces.

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

b. Qualitative MOEs

(1) Attitude of a target population to a specific issue as gauged by a survey or poll.

(2) Number of surrendering troops as a result of a PSYOP leaflet campaign.

(3) Effectiveness of a mine awareness campaign as measured by the number of mine strikes against the target population.

CHAPTER VI
MULTINATIONAL CONSIDERATIONS IN INFORMATION OPERATIONS

NOTE: The following is a complete rewrite of old Chapter VIII from the First Draft.

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

George C. Marshall

1. Introduction

Joint doctrine for multinational operations, including command and operations in a multinational environment, is set out 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, Dec 01, Chapter 10. This document includes useful IO checklists for staff and commanders assigned to a multinational or coalition 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 operations. The multinational force commander (MFC) 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. Initial requirements for integration of other nations into the IO effort include:

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

(2) Understanding of other national information operations and how they intend to conduct IO.

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

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

b. Regardless of the maturity of each nation's IO capabilities, doctrine, and/or TTP, **every ally/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 a way that US capabilities are not. **Such contributions complement United States 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' ROE and legal constraints concerning military activities in the information dimension.

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

(6) Familiarity with allied/coalition partner IO doctrine or TTP.

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 operation. 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. The optimal solution to the difficult problem of sharing classified information among countries must include training and education on established procedures.

(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 CJCSI 6510.01, *Information Assurance (IA) and Computer Network Defense (CND)*, 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. 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. However, the JFC should request approval from higher command authorities for IO-related information that has not been cleared with allied/coalition partners.

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 MFC. The mission of the multinational force determines the role of IO in each specific operation.

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

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

5. Multinational Organization for Information Operations Planning

a. When the JFC is also the MFC, 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 MFC, it may be necessary for **the JFC J-3 to brief the MFC and staff on the advantages of using US IO capabilities and procedures to achieve multinational force goals**. The JFC should propose organizing a multinational IO staff using organizational criteria discussed earlier. If this is not acceptable to the MFC, 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, TTP, plans, intelligence, and C4 support applicable to IO requires coordination with the responsible DOD components and allied/coalition nations. Coordination with allies above the JFC/MFC level will normally be effected within existing defense arrangements, including the use of bilateral arrangements. **The Joint Staff, with the support of USSTRATCOM, coordinates United States positions on all IO matters** 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.

Intentionally Blank

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

NOTE: The following is a complete rewrite of old Chapter IX from the First Draft.

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

1. Introduction

The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities at all level 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, is 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 framework of education and training requirements necessary for an IO career force include:

a. **The IO career force should consist of both capability specialists (EW, PSYOP, and CNO) 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 MILDEC and OPSEC to ensure integration of IO into joint operations.

b. **Initial capability specialist training and education requirements are Service and capability specific.** Capability specialist may be officers or enlisted. As Service-trained specialist 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 train those personnel and organizations responsible for planning and conducting joint IO in the concepts and doctrine found in this and other joint policies and doctrine.**

b. **IO training must support the IO career force and be consistent with the joint assignment process.** The operational tempo at joint commands is normally too high for newly assigned personnel to attend training that is not command specific once they report for permanent duty. **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 seamless nature of the information environment** and the fact that the **actions of individual personnel affect the perceptions of foreign populations and can have second and third order effects that are potentially strategic in scope**. 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 stationed or assigned to overseas locations where cultural values and institutions differ substantially from the United States 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 United States forces' actions and conduct by foreign populations where deployed.** Personnel expected to operate at length or covertly among foreign populations must receive more extensive cultural training.

(2) **Language skills are important to IO.** Language training in the past has focused on intelligence requirements. IO requires not only that appropriate messages and themes be translated accurately, but that joint forces have the language 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 skills to communicate effectively with the populations they operate among.** The burden of acquiring proficiency in a foreign language cannot be expected to fall primarily on the foreign population's ability to learn English. **Lack of**

sufficient language expertise makes the joint force dependent on foreign translators. Language training must provide sufficient numbers of personnel fluent in those languages where joint forces expect to operate for those forces to interact effectively with foreign populations and maintain awareness of foreign population perceptions during the course of all types of joint operations.

(3) **Specific IO capabilities, such as CND, OPSEC, and physical security, also have training requirements that are applicable to the general military population on a continuing basis.** Such capabilities are 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 capabilities in the overall IO effort and their impact on the conduct of joint operations. Such in-depth training requires reinforcement and enhancement throughout their careers. Only this depth and 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 that complement and enhance the conduct of military activity in the physical domains.

4. Planning Information Operations in Joint Exercises

Effective employment of IO in joint operations depends on the ability of United States 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 the 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 classified SIPRNET.

(1) More information about the joint training program can be obtained from CJCSM 3500.03, *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) **Developing an IO concept of operations** (for "Blue" and "Red" forces) that is integrated into the JFC's concept of operations.

(c) **Coordinating IO personnel and assets** to participate as both "Blue" 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" participants.

(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 such as 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' Commended Training Issues for applicable objectives.

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

(3) 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.

(4) The number and type of IO capabilities and personnel that will be appropriate for the type of exercise and its objectives.

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

(6) **Defining exercise "play" area(s) in the information environment.** The seamlessness of 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 if not properly "confined." Fires that have effect in the information dimension from CNA or EA exercise activity have the potential to affect or "interact" with the information dimension outside the designated exercise area. Exercise planners should specifically evaluate the potential for such 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.

(7) **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.

(8) The type of M&S systems that will be used as part of the exercise.

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

(10) **Evaluation of possible adverse effect 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 United States capabilities, tactics, 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) **Development of specific, attainable IO exercise objectives.** IO exercise objectives are statements of anticipated effects that result from specific IO actions. The identification and accomplishment of these objectives will 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) **Provide the opportunity for sufficient military information activity to test the abilities of IO planners to coordinate such 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 requires detailed and careful thought. Assumptions must be made about friendly and adversary IO capabilities, baseline perceptions of appropriate individuals and groups, and how perceptions may change over the course of the exercise in reaction to ALL scripted events and in reaction to exercise play.

Baseline perception and IO-related intelligence must be provided in documentation that both Blue and Red forces receive at start of exercise (STARTEX). Technical and safety requirements for EA and CNA 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) Availability of IO assets during exercise play must support training objectives. 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 loss of exercise assets to operational requirements.

(5) Scripting appropriate IO-related events for the MSEL is a critical and time-consuming process. It requires extensive IO knowledge. 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) **Create as realistic an exercise environment as possible.** For training purposes the information environment in an exercise should be as realistic 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 in conducting strategic influence campaign planning or DSPD.

(7) **Ensure adequate manning for IO staff functions and IO evaluations.** 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) **Ensure that "real world" OPSEC is considered in the exercise planning effort.** 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 efforts of hostile intelligence systems.

(9) **Coordinate the use of simulations 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 IPB 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 the IO aspects of the exercise should focus their efforts on ensuring that the IO events in the MSEL occur as planned, that actual IO exercise activities remain focused on the training objectives, and that data and observations which support 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 will instruct, who will attend, 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 is 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 process provides the means to conduct structured analysis of specific IO TTP and capabilities in a controlled environment. This process is crucial to establishing, gauging, and validating proposed IO TTP and capabilities in order to allocate scarce 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 joint experimentation. USJFCOM develops the joint experimentation (JE) campaign plan and coordinates it though Joint Staff J-7, with the combatant commanders, Services, Joint Staff, OSD, and Defense agencies. USJFCOM submits the JE campaign plan for CJCS approval through the Joint Requirements Oversight Council (JROC) process (to include 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*, Enclosure B, "Joint Requirements Oversight Council Programmatic Process for Joint DOTMLPF 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 BETWEEN INFORMATION OPERATIONS CORE CAPABILITIES

SUPPORTED → / SUPPORTING ↓	EW	CNO	PSYOP	MILDEC	OPSEC
ELECTRONIC WARFARE (EW)		Supplementing computer network attack (CNA) with electronic attack (EA) Using electronic protection (EP) to protect personnel, facilities, and equipment	Degrading adversary's ability to see, report, and process information Isolating target audience from information	Using EA/electronic warfare support (ES) as deception measures Degrading adversary capabilities to see, report, and process competing observable	Degrading adversary electromagnetic intelligence, surveillance, and reconnaissance operations against protected units and activities
COMPUTER NETWORK OPERATIONS (CNO)	Used with EA Used in conjunction with EP		Another means of delivering PSYOP messages Preventing the compromise of PSYOP message before release	Providing the deception through computers and protecting the MILDEC plan resident inside computers	Detecting and preventing adversary attempts to acquire information
PSYCHOLOGICAL OPERATIONS (PSYOP)	Broadcasting PSYOP products on adversary frequencies	Convincing adversary not to do something by describing effects of a CNA if they take undesirable actions		Creating perceptions and attitudes that MILDEC can exploit Reinforcing the deception story with information from other sources	Countering propaganda and misinformation Minimizing resistance and interference by local population
MILITARY DECEPTION (MILDEC)	Influencing adversary to underestimate friendly EA/ES capabilities	Providing MILDEC targets and deception stories for CNA Causing adversary to expose systems to CNO	Providing information compatible with PSYOP theme		Distract adversary collection assets
OPERATIONS SECURITY (OPSEC)	Concealing EW units and systems to deny information on extent of EA/ES capabilities	Concealing CNA/computer network defense capabilites	Concealing contradicting indicators	Concealing observables Degrading general situation information to enhance effect of observables	

Figure B-1. Mutual Support Between Information Operations Core Capabilities

Intentionally Blank

APPENDIX C
REFERENCES

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

1. Executive Branch Documents

a. *National Security Strategy.*

b. *Unified Command Plan FY 02* (through Chg 2).

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, ~~*DOD*~~ *Electronic Warfare (EW) and Command and Control Warfare(C2W) Countermeasures.*

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

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

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

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

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

~~h. DODD 5240.6, *Counterintelligence Awareness Briefing Program.*~~

h. DODD ~~O~~-8500.1, *Information Assurance* *(IA)*.

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

j. DODI S-3600.2, *Information Operations* ~~*(IO)*~~ *Security Classification Guidance.*

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

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

m. DODI 5240.10, *DOD Counterintelligence Support to Unified and Specified Commands.*

n. DODI ~~O~~ 8500.2, *Information Assurance(IA) Implementation.*

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

p. *National Military Strategy* (2004).

4. Joint Policy, Doctrine, and Other Publications

a. CJCSI 1800.01A, *Officer ~~PME~~ Professional Military Education Policy.*

b. CJCSI 3110.05C~~B~~, *Joint Psychological Operations Supplement to the Joint Strategic Capabilities Plan FY ~~1998~~2002.*

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

d. CJCSI 3141.01A, *Responsibilities for the Management and Review of ~~OPLANS~~Operation Plans.*

e. CJCSI 3150.25A, *Joint ~~After-Action Reporting System~~ Lessons Learned Program.*

f. CJCSI 3170.01D, *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 ~~Applicable to All Combatant Commands~~.*

h. CJCSI 3210.01A, *Joint Information Operations Policy ~~for IO~~.*

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

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

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

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

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

~~n. CJCSM 3141.01, *Procedures for Review of Operations Plans.*~~

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 (JOPES) 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 3500.04C, *Universal Joint Task List (UJTL).*

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

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

~~y. CJCS Notice 3502, *Quarterly Schedule of Significant Military Exercises.*~~

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 2-01.1, *Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting.*

cc. JP 2-01.2, *Joint Doctrine, Tactics, Techniques, and Procedures for ~~CI~~ Counterintelligence Support to Operations (U).*

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

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

ff. JP 3-01.4, *Joint Tactics, Techniques, and Procedures for Joint Suppression of Enemy Air Defenses (J-SEAD).*

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

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

ii. JP 3-08, *Interagency Coordination During Joint Operations Vol. 1.*

jj. JP 3-08, *Interagency Coordination During Joint Operations Vol. 2.*

kk. JP 3-09, *Doctrine for Joint Fire Support.*

ll. JP 3-10, *Joint Doctrine for Rear Area Operations.*

mm. JP 3-10.1, ~~*JTTP*~~ *Joint Tactics, Techniques, and Procedures for Base Defense.*

nn. JP 3-13, *Joint Doctrine for Information Operations.*

oo. JP 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W).*

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

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

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

ss. JP 3-51, *Joint Doctrine for Electronic Warfare.*

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

uu. JP 3-54, *Joint Doctrine for Operations Security.*

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

ww. JP 3-58, *Joint Doctrine for Military Deception.*

xx. JP 3-60, *Joint Doctrine for Targeting.*

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

zz. JP 5-0, *Doctrine for Planning Joint Operations*.

aaa. JP 5-00.1, *Joint Doctrine for Campaign Planning.*

bbb. JP 5-00.2 *Joint Task Force ~~(JTF)~~ Planning Guidance and Procedures.*

ccc. JP 6-0, *Doctrine for C4 Systems Support to Joint Operations.*

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

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

5. Multiservice and Service Publications

a. JTF-IM**,** *Multiservice Procedures for Joint Task Force-Information Management.*

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

c. *Information Operation Primer* United States Army War College.

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

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

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

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

6. Books, Papers, and Articles

a. *Webster's Third New International Dictionary, Unabridged*. Merriam-Webster, 2002.

b. Bloom, Bradley, Lieutenant Colonel, United States Army. *Information Operations in Support of Special Operations*, Military Review January – February 2004.

c. Burnett, Peter L., Lieutenant Colonel, United States Army (2002). *Information Operations* Strategy Research Project United States Army War College Carlisle Barracks.

d. *Changing Minds Winning Peace A New Strategic Direction for U.S. Public Diplomacy in the Arab & Muslim World* (2003) Report of the Advisory Group on Public Diplomacy for the Arab and Muslim World Edward P. Djerejian Chairman.

~~e. Davis, Paul K., Draft Monograph. *Effects Based Operations (EBO): A Grand Challenge to the Analytic Community* (Rand National Defense Research Institute and Project Air Force MR-1477-USJFCOM/AF).~~

e. DeMattei, Lou Anne, Commander, United States Navy (2004). *Information Operations Doctrine: Service Perspectives* Joint Forces Staff College Advanced Joint Professional Military Education Paper.

f. Defense Science Board Task Force on Defensive Information Operations (2001). *Protecting the Homeland*, Summer Study Report 2000 Volume II Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics.

g *Finding America's Voice: A Strategy for Reinvigorating U.S. Public Diplomacy* (2003), the report of an independent task force sponsored by the Council on Foreign Relations.

h. Mayer, James T., Major, United States Army, *The Employment of a Web Site and Web Enabling Technology in Support of U.S. Military Information* Operations Naval Postgraduate School Thesis.

i. LaWarren V. Patterson, Lieutenant Colonel, United States Army (2002). *Information Operations and Asymmetric Warfare…Are We Ready?* Strategic Research Project, United States Army War College Carlisle Barracks.

j. Thrasher, Roger Dean (1996). *Information Warfare Delphi: Raw Results* Naval Postgraduate School.

k. Williamson, Jennie M., Lieutenant Colonel, United States Army (2002). *Information Operations: Computer Network Attack in the 21st Century* Strategic Research Project United States Army War College Carlisle Barracks.

APPENDIX D
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

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

2. Authorship

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

3. Supersession

This publication supersedes JP 3-13, 9 October 1998, *Joint Doctrine for Information Operations*.

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//
USJFCOM NORFOLK VA//JW100//

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

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

c. Record of Changes:

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

5. Distribution

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

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, 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*.

Army:	US Army AG Publication Center SL 1655 Woodson Road Attn: Joint Publications St. Louis, MO 63114-6181
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Commander (Attn: Publications) 814 Radford Blvd, Suite 20321 Albany, GA 31704-0321
Coast Guard:	Commandant Coast Guard (G-OPD), US Coast Guard 2100 2nd Street, SW Washington, DC 20593-0001
	Commander USJFCOM JWFC Code JW2102 Doctrine Division (Publication Distribution) 116 Lake View Parkway Suffolk, VA 23435-2697

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

1
2

Intentionally Blank

GLOSSARY
PART I — ABBREVIATIONS AND ACRONYMS

AAR	~~after-action~~ after action report
~~ADCON~~	~~administrative control~~
~~AFDD~~	~~Air Force doctrine document~~
~~AFIWC~~	~~Air Force Information Warfare Center~~
~~AI~~	~~artificial intelligence~~
AOR	area of responsibility
ATO	air tasking order
BDA	battle damage assessment
~~BDOC~~	~~base defense operations center~~
C2	command and control
~~C3I~~	~~command, control, communications, and intelligence~~
C4	command, control, communications, and computers
CA	civil affairs
~~CCTI~~	~~Chairman of the Joint Chiefs of Staff commended training issue~~
~~CDRUSCENTCOM~~	~~Commander, United States Central Command~~
CDRUSSOCOM	Commander, United States Special Operations Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CI	counterintelligence
~~CIOTA~~	~~counterintelligence operational tasking authority~~
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
COCOM	combatant command (command authority)
COG	center of gravity
COMCAM	combat camera
COMSEC	communications security
CONPLAN	operations plan in concept format
~~CTP~~	~~common tactical picture~~
~~D3A~~	~~decide, detect, deliver, and assess~~
~~DCTS~~	~~Defense Collaborative Tool Suite~~
~~DDGO~~	~~Joint Staff J-3 Deputy Director Global Operations~~
~~DDIO~~	~~Joint Staff J-3 Deputy Director Information Operations~~

~~DE~~	~~directed energy~~
DIA	Defense Intelligence Agency
~~DII~~	~~defense information infrastructure~~
~~DIRLAUTH~~	~~direct liaison authorized~~
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOS	Department of State
~~DOTMLPF~~	~~doctrine, organization, training, material, leadership and education, personnel, and facilities~~
~~DPG~~	~~Defense Planning Guidance~~
DPO	Joint Program Office for Special Technology Countermeasures
DSPD	defense support to public diplomacy
EA	electronic attack
~~ECP~~	~~exercise control plan~~
EEFI	essential elements of friendly information
EM	electromagnetic
~~EMCON~~	~~emission control~~
~~EMI~~	~~electromagnetic interference~~
EP	electronic protect
ES	electronic warfare support
EW	electronic warfare
EWCC	electronic warfare coordination cell
~~FHA~~	~~foreign humanitarian assistance~~
~~FM~~	~~field manual~~
FPC	final planning conference
GIG	Global Information Grid
~~GO/FO~~	~~general officer/flag officer~~
~~HN~~	~~host nation~~
HQ	headquarters
~~HSS~~	~~health service support~~
~~HUMINT~~	~~human intelligence~~
IA	information assurance
~~IAM~~	~~information assurance manager~~
~~IAO~~	~~information assurance officer~~
IC	intelligence community
IM	information management
~~INFOCON~~	~~information operations condition~~
INFOSEC	information security
IO	information operations

~~ION~~	~~Information Operations Navigator~~
~~IOS~~	~~IO squadron~~
~~IOTC~~	~~Information Operations Technology Center~~
IPB	intelligence preparation of the battlespace
IPC	initial planning conference
~~ISR~~	~~intelligence, surveillance, and reconnaissance~~
IT	information technology
~~IWPC~~	~~Information Warfare Planning Capability~~
~~IWS~~	~~Information Work Space~~
J-2	intelligence directorate of a joint staff
~~J-2T~~	~~joint force intelligence directorate deputy director for targets~~
~~J-2X~~	~~joint force intelligence directorate counterintelligence and human intelligence staff element~~
J-3	operations directorate of a joint staff
J-4	logistics directorate of a joint staff
~~J-5~~	~~plans directorate of a joint staff~~
J-6	command, control, communications, and computer systems directorate of a joint staff;
J-7	operational plans and joint force development directorate of a joint staff
~~J-9~~	~~civil-military operations staff section~~
JA	Judge Advocate
JCCC	joint communications control center
~~JCEWS~~	~~joint force commander's electronic warfare staff~~
JCMA	joint communications security (COMSEC) monitor activity
~~JCS~~	~~Joint Chiefs of Staff~~
JCSE	joint communications support element
JE	joint experimentation
~~JECG~~	~~joint exercise control group~~
JFC	joint force commander~~s~~
~~JFMO~~	~~Joint Frequency Management Office~~
~~JIB~~	~~joint information bureau~~
JIOAPP	joint information operations attack planning process
~~JIOC~~	~~joint information operations center~~
JIODPP	joint information operations defensive planning process
JIOPP	joint information operations planning process
~~JISE~~	~~joint intelligence support element~~
~~JMETL~~	~~joint mission essential task list~~
JOA	joint operations area
JOC	joint operations center
JOPES	Joint Operations Planning and Execution System
JP	joint publication
JPG	joint planning group
~~JPO-STC~~	~~Joint Program Office for Special Technology Countermeasures~~

JPOTF	joint psychological operations task force
~~JRB~~	~~Joint Requirements Oversight Council (JROC) Review Board~~
JRFL	joint restricted frequency list
JROC	Joint Requirements Oversight Council
~~JRTOC~~	~~joint rear tactical operations center~~
JSC	Joint Spectrum Center
JTCB	joint targeting ~~control~~ coordination board
JTF	joint task force
~~JULLS~~	~~Joint Universal Lessons Learned System~~
JWAC	Joint Warfare Analysis Center
~~LAN~~	~~local area network~~
LOAC	law of armed conflict
M&S	modeling and simulation
MASINT	measurement and signature intelligence
~~MCA~~	~~military civic action~~
MFC	multinational force commander
MILDEC	military deception
MOE	measure~~s~~ of effectiveness
~~MOOTW~~	~~military operations other than war~~
~~MP~~	~~military policy~~
MPC	mid-planning conference
MSEL	master scenario events list
~~MSPD~~	~~military support to public diplomacy~~
NETOPS	network operations
~~NIWC~~	~~Naval Information Warfare Center~~
NGO	nongovernmental organization
~~NPS~~	~~Naval Postgraduate School~~
NSA	National Security Agency
~~NWP~~	~~naval warfare publication~~
OA	orientation activities
OPB	operational preparation of the battlespace
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSD	Office of Secretary of Defense
~~OT&E~~	~~operational test & evaluation~~
PA	public affairs
~~PAO~~	~~public affairs officer~~
PD	public diplomacy

PIR	priority intelligence requirement
~~PME~~	~~professional military education~~
POAT	psychological operations assessment team
~~PSE~~	~~psychological operations support element~~
PSYOP	psychological operations
~~R&D~~	~~research and development~~
RFI	request for information
ROE	rules of engagement
SecDef	Secretary of Defense
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
~~SJA~~	~~Staff Judge Advocate~~
SJF	standing joint force
SME	subject matter expert~~s~~
SOF	special operations force
SOP	standing operating procedure
STARTEX	~~exercise~~ start of exercise
STO	special technical operations
TA	target audience
~~TACON~~	~~tactical control~~
~~TEPS~~	
TPFDD	time-phased force and deployment data
TPFDL	time-phased force and deployment list
TSCP	theater security cooperation plan
TTP	tactics, techniques, and procedures
~~UCP~~	~~Unified Command Plan~~
UJTL	Universal Joint Task List
~~USA~~	~~United States Army~~
~~USAF~~	~~United States Air Force~~
~~USCG~~	~~United States Coast Guard~~
USG	United States Government
USJFCOM	United States Joint Forces Command
~~USMC~~	~~United States Marine Corps~~
~~USN~~	~~United States Navy~~
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command

PART II — TERMS AND DEFINITIONS

~~**airspace control authority.** (DOD, NATO) The commander designated to assume overall responsibility for the operation of the airspace control system in the airspace control area. Also called ACA. See also airspace control; airspace control area; airspace control system; control; operation.~~

~~**airspace control in the combat zone.** A process used to increase combat effectiveness by promoting the safe, efficient, and flexible use of airspace. Airspace control is provided in order to prevent fratricide, enhance air defense operations, and permit greater flexibility of operations. Airspace control does not infringe on the authority vested in commanders to approve, disapprove, or deny combat operations. Also called airspace control; combat airspace control. (JP 1-02)~~

air tasking order. ~~(DOD)~~ 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 United States objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. 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)

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 system.** The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JP 1-02)~~

command and control warfare. ~~command and control warfare The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.~~ None. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will be removed from 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. Also called COMSEC. Communications security includes: crypto security, transmission security, emission security, and physical security of communications security materials and information. a. crypto security — The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. transmission security — The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. emissions security — The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. physical security — The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

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

computer intrusion detection. The process of identifying that a computer intrusion has been attempted, is occurring, or has occurred. (JP 1-02)

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks.~~, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA.~~ Also called CNA. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

computer network defense. Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and computer networks. ~~CND is an operational component of Information Assurance and a core capability component of IO. CND employs IA to include deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information.~~ Also called CND. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

computer network exploitation. ~~Enabling operations and i~~Intelligence collection ~~to~~ which gathers data from target or adversary automated information systems or networks. Also

called CNE. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will be included in JP 1-02.)

computer network operations. Comprised of computer network attack, computer network defense, ~~CNA, CND,~~ and related ~~CNE~~ computer network exploitation enabling operations. Also called CNO. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will be included in JP 1-02.)

~~**computer security.** The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. Also called COMPUSEC. (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)

~~**critical node** — An element, position, or command and control entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations. Also called target critical damage point. (JP 1-02)~~

~~**cyber counterintelligence** — Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligences service collection efforts that use traditional methods to gauge cyber capabilities and intentions. See also counterintelligence. (JP 1-02)~~

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)

~~**deconfliction.** The process of coordination among organizations or their subdivisions to avoid incompatibility, irreconcilability, or opposition when two or more military forces or capabilities are employed simultaneously or in particular sequence during military operations. (Upon approval of the revision of this publication, this term and its definition will be included in JP 1-02.)~~

~~**military** **defense** **support to public diplomacy.** Those activities and measures taken by the ~~DOD~~ Department of Defense components to support and facilitate public diplomacy. Also called DSPD. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will be included in 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)

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. Also called EW. (JP 1-02)

emission control. The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan. Also called EMCON. See also electronic warfare. (JP 1-02)

~~**fire control.** (DOD, NATO) The control of all operations in connection with the application of fire on a target. (JP 1-02)~~

fires. The effects of lethal or nonlethal weapons. (JP 1-02)

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)

Global Information Grid. ~~(DOD)~~ 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 (GIG) includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense (DOD), National Security, and related intelligence community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.~~ Also called GIG. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

human factors. 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. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will be included in 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. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (JP 1-02)

~~**information fires.** Nonlethal and nonkinetic effects, including psychological, electromagnetic, or cyber capabilities, employed by military or terrorist organizations as force or threat of force as such organizations have historically employed force in the physical dimensions (land, sea, air, and space). (Upon approval of the revision of this publication, this term and its definition will be included in JP 1-02.)~~

~~**information management.** The planning, budgeting, manipulating, and controlling of information throughout its life cycle. (Upon approval of the revision of this publication, this term and its definition will be included in JP 1-02.)~~

~~**information maneuver.** The deliberate positioning of information in military operations for presentation to target audiences. (Upon approval of the revision of this publication, this term and its definition will be included in 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. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in 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. ~~Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.~~ Also called INFOSEC. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

information superiority. ~~The capabilities to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.~~ That degree of dominance in the information ~~domain~~ dimension which permits the conduct of

operations without effective opposition. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will modify the existing term and its definition and be included in JP 1-02.)

information system. The entire infrastructure, organization, personnel, and components ~~that~~ for the collection, processing, ~~store~~storage, transmission, ~~transmit,~~ display, ~~and disseminate~~ dissemination, and disposition of information. (~~Approved for inclusion~~ Upon approval of this revision, this term and its definition will be included in the next edition of JP 1-02.)

information warfare. None. (Upon approval of this revision, this term and its definition will be removed from 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 ~~0-2~~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)

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 intelligence preparation of the battlespace.** The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's decision making process. It is a continuous process that includes defining the total battlespace environment; describing the battlespace's effects; evaluating the adversary; and determining and describing adversary potential courses of action. The process is used to analyze the air, land, sea, space, electromagnetic, cyberspace, and human dimensions of the environment and to determine an opponent's capabilities to operate in each. Joint intelligence preparation of the battlespace products are used by the joint force and component command staffs in preparing their estimates and are also applied during the analysis and selection of friendly courses of action. Also called JIPB. (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. (Upon approval of this revision, this term and its definition will be removed from JP 1-02.)

military deception. Those measures designed to mislead an adversary by manipulation, distortion, or falsification to induce him to react in a manner prejudicial to his interest. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are ~~as follows. a.~~ strategic military deception, ~~— Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations. b.~~ operational military deception, ~~— Military deception planned and executed by and in support of operational level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater to support campaigns and major operations. c.~~ tactical military deception, ~~— Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. d.~~ Service military deception, and ~~— Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems. e.~~ military deception in support of operations security ~~(OPSEC).~~ ~~— Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities.~~ Also called MILDEC. See also deception. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

~~**movement control.** (DOD) 1. The planning, routing, scheduling, and control of personnel and cargo over lines of communications. (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)

operational preparation of the battlespace. Non-intelligence activities conducted to plan and prepare for potential follow-on military operations, conducted under Title 10 authority. Also called OPB. (Upon approval of this revision, this term and its definition will be included in the next edition of 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. ~~physical security (*)~~ That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. See also communications security~~; security~~. (JP 1-02)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (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. ~~Also called PD.~~ (JP 1-02)

reachback. ~~(DOD)~~ 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 United States 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 United States and friendly space systems; prevention of an adversary's ability to use space systems and services for purposes hostile to United States

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

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. (JP 1-02)

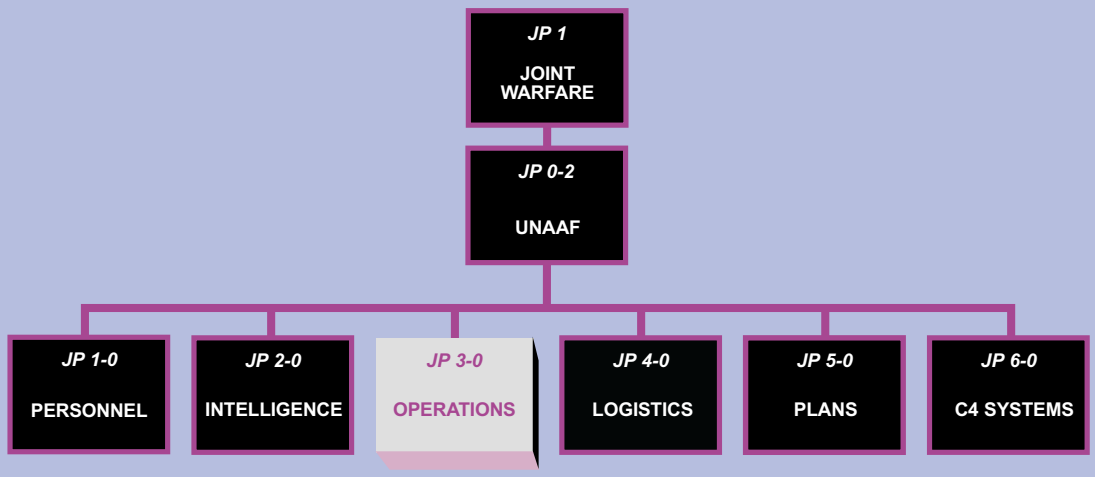
strategic communication. The transmission of integrated and coordinated United States Government themes and messages that advance United States interests and policies through a synchronized interagency effort that includes public diplomacy, public affairs, and information operations, in concert with other political, economic, and military actions. (Upon approval of the revision of this publication, this term and its definition will modify the existing term and definition and be included in 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)

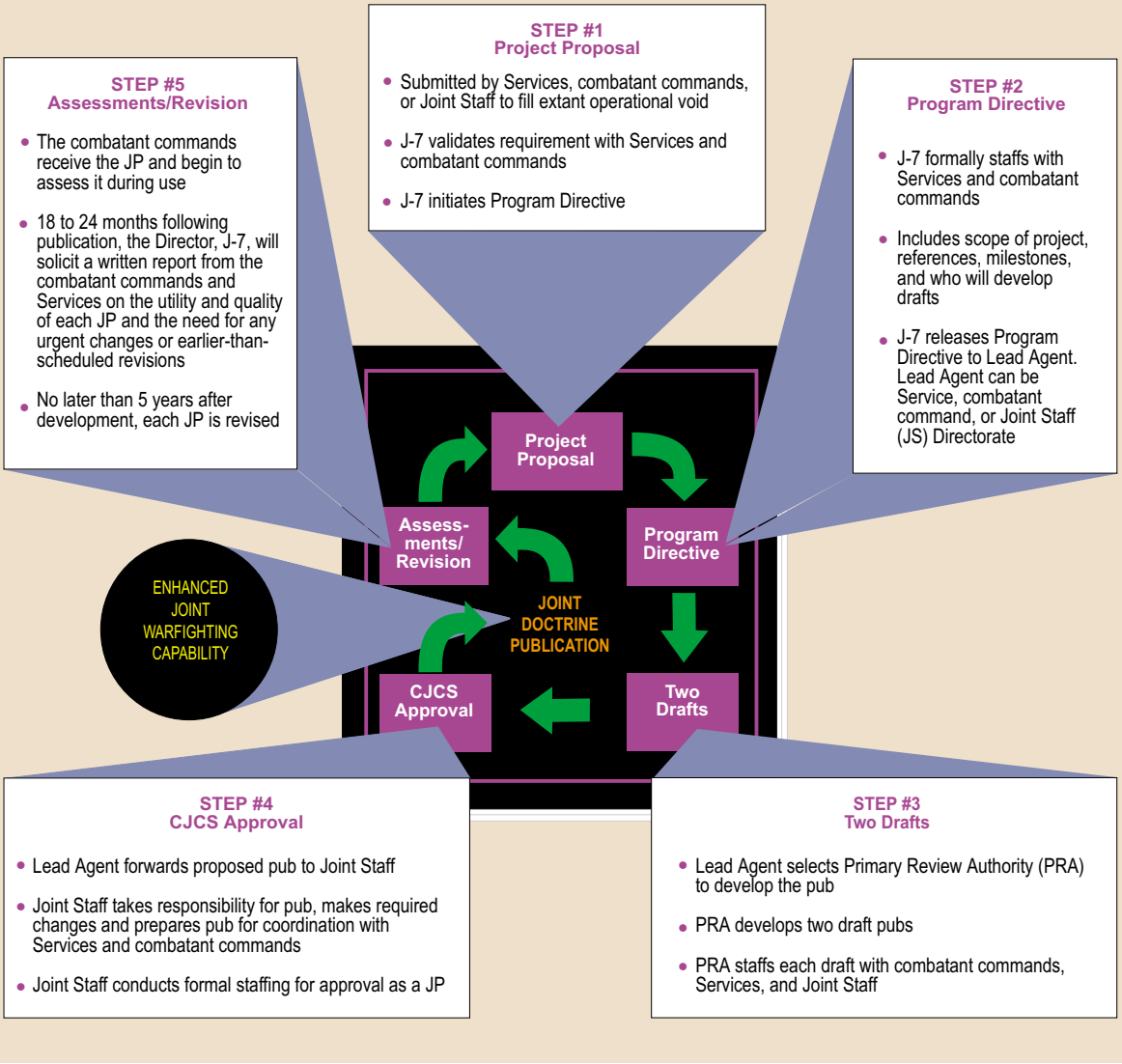
target audience. ~~(*)~~ An individual or group selected for influence or attack by means of psychological operations. Also called TA. (Upon approval of ~~the~~ this revision ~~of this publication~~, this term and its definition will modify the existing term and its definition and be included in JP 1-02.)

vulnerability analysis. None. (Upon approval of this revision, this term and its definition will be removed from JP 1-02.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are 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