FM 3-13 (FM 100-6)

Information Operations: Doctrine, Tactics, Techniques, and Procedures

NOVEMBER 2003

HEADQUARTERS, DEPARTMENT OF THE ARMY

Field Manual
No. 3-13

Headquarters
Department of the Army
Washington, DC, 28 November 2003

Information Operations: Doctrine, Tactics, Techniques, and Procedures

Contents

*This publication supersedes FM 100-6, 27 August 1996.

Preface

Information is an element of combat power. Commanders conduct information operations (IO) to apply it. Focused IO—synchronized with effective information management and intelligence, surveillance, and reconnaissance—enable commanders to gain and maintain information superiority. IO is a prime means for achieving information superiority.

Users of FM 3-13 must be familiar with the military decisionmaking process established in FM 5-0, *Army Planning and Orders Production*; the operations process, established in FM 3-0, *Operations*; and commander's visualization, described in FM 6-0, *Mission Command: Command and Control of Army Forces.*

PURPOSE

As the Army's key integrating manual for IO, this manual prescribes IO doctrine and tactics, techniques, and procedures (TTP). It also establishes doctrine and TTP for the IO elements of operations security and military deception. This manual implements joint IO doctrine established in JP 3-13, *Joint Doctrine for Information Operations*; JP 3-54, *Joint Doctrine for Operations Security*; and JP 3-58, *Joint Doctrine for Military Deception*.

This manual establishes the following as the definition of IO used by Army forces: ***Information operations*** **is the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decisionmaking.** This definition supersedes the definition of IO in FM 3-0. It is consistent with joint initiatives.

SCOPE

The publication addresses IO doctrine in Part I and TTP in Part II. Part I also establishes Army operations security (OPSEC) and military deception doctrine.

APPLICABILITY

This publication applies to Army forces from Army service component command (ASCC) to maneuver brigade. It is most applicable to corps and divisions. The primary users of this manual are ASCC, corps, division, and brigade commanders and staff officers—specifically the G-2, G-3, G-7, and staff representatives for military deception, electronic warfare, operations security, fire support, psychological operations, civil affairs, and public affairs. Battalions normally execute higher headquarters IO. In stability operations and support operations, they may be given IO assets. Thus, they need to know their role in brigade and division IO.

TRADOC service schools and branch proponents should use FM 3-13 as a point of departure for integrating IO into branch doctrine and military instruction.

ADMINISTRATIVE INFORMATION

Terms that have joint or Army definitions are identified in both the glossary and the text. The glossary lists most terms used in FM 3-13 that have joint or Army definitions. Terms for which FM 3-13 is the proponent manual (the authority) are indicated with an asterisk in the glossary. Definitions for which FM 3-13 is the proponent manual are printed in boldface in the text. These terms and their definitions will be incorporated into the next revision of FM 1-02. For other definitions in the text, the term is italicized and the number of the proponent manual follows the definition.

The glossary contains referents of acronyms and definitions of terms not defined in JP 1-02 and FM 1-02. It does not list acronyms and abbreviations that are included for clarity only and appear one time, nor those that appear only in a figure and are listed in the legend for that figure. Some common abbreviations and acronyms—for example, the abbreviations for military ranks and publications—are not spelled out; refer to the glossary. Since *ARFOR* is a defined term as well as an acronym, it is not spelled out.

"President" refers to the President and the Secretary of Defense, or their duly deputized alternates and successors.

All references to annexes refer to annexes to operation plans (OPLANs) or operation orders (OPORDs) unless stated otherwise.

Unless stated otherwise, masculine nouns or pronouns do not refer exclusively to men.

Headquarters, US Army Training and Doctrine Command, is the proponent for this publication. The preparing agency is the Combined Arms Doctrine Directorate, US Army Combined Arms Center. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: Commander, US Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-CD (FM 3-13), 1 Reynolds Road (Building 111), Fort Leavenworth, KS 66027-1352. Send comments and recommendations by e-mail to web-cadd@leavenworth.army.mil. Follow the DA Form 2028 format or submit an electronic DA Form 2028.

Introduction

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

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

Commanders do not conduct IO simply for the sake of doing IO. Effective IO is an integrated effort that synchronizes the effects of IO elements/related activities to accomplish specific objectives designated by the commander. It is the means commanders use to mass the effects of the information element of combat power.

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

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

The goal of IO is to gain and maintain information superiority, a condition that allows commanders to seize, retain, and exploit the initiative. It facilitates more effective decisionmaking and faster execution. IO involve constant efforts to deny adversaries the ability to detect and respond to friendly operations, while simultaneously retaining and enhancing friendly force freedom of action. When expeditiously exploited, IO provide a potent advantage that facilitates rapid military success with minimal casualties. Effective IO and information management allow commanders to take advantage of opportunities, while denying adversary commanders the information needed to make timely and accurate decisions or leading them to make decisions favorable to friendly forces.

Army forces routinely employed the elements of IO separately in past conflicts. Psychological operations, operations security, military deception, physical destruction, and electronic warfare were viable tools of Army commanders during World War II. The Gulf War demonstrated the benefit of employing these elements

together and synchronizing them with ground operations. Capitalizing on this knowledge, the Joint Staff produced a series of doctrinal publications that culminated in October 1998 with JP 3-13, *Joint Doctrine for Information Operations*.

Today, Army IO doctrine and tactics, techniques, and procedures (TTP) adapt joint IO doctrine to achieve information superiority at decisive points during full spectrum operations. Because adversaries have asymmetric abilities to counter finite friendly IO capabilities, the probability of maintaining information superiority over long periods is unlikely. Therefore, commanders execute IO to gain information superiority at times and places where it supports their intent and concept of operations.

Technological advancements in automated INFOSYS and communications have allowed commanders to see the battlefield as actions unfold, closer to near real-time than ever before, and to rapidly pass information across their areas of operations. Combined, IO and advanced INFOSYS and communications continue to shorten the time required for staff processes. This compresses the decision cycle and increases operational tempo, the rate of military action. Commanders now have opportunities to achieve decisive results early in an operation, reducing casualties and conserving resources.

Advancements in automated INFOSYS and communications carry with them vulnerabilities commanders need to recognize and offset. Clearly, a force dependent on technology offers adversaries new opportunities to degrade its effectiveness. Army forces face significant vulnerabilities due to their dependence on information technology. Army communications and technologies are becoming more and more dependent on commercial backbones and commercial off-the-shelf products and systems that are also readily available to potential adversaries. This situation makes defensive IO an essential aspect of all operations.

PART ONE

Information Operations Doctrine

Commanders conduct (plan, prepare, execute, and assess) information operations (IO) to apply the information element of combat power. Combined with information management and intelligence, surveillance, and reconnaissance operations, effective IO results in gaining and maintaining information superiority. Information superiority creates conditions that allow commanders to shape the operational environment and enhance the effects of all elements of combat power. IO has two categories, offensive IO and defensive IO. Commanders conduct IO by synchronizing IO elements and related activities, each of which may be used either offensively or defensively. Army IO doctrine supports joint IO doctrine, supplementing it where necessary to meet the conditions of land operations. Part One discusses the doctrinal concepts that underlie IO and the capabilities of, contributions made by, and links among the IO elements and related activities. It also establishes doctrine for two IO elements: operations security and military deception.

Chapter 1

Design of Army Information Operations

Information operations (IO) bring together several previously separate functions as IO elements and related activities. To provide unity of effort, IO is placed under a special staff officer, the assistant chief of staff G-7.

CONTENTS

The G-7 has coordinating staff responsibility for IO. He does this by means of the G-7 section and IO cell. Placing responsibility for synchronizing the activities of the IO elements and related activities on one special staff officer helps commanders mass their effects to gain and maintain information superiority. Chapter 1 discusses the role of the G-7 and IO cell. In addition, it describes the information environment (where Army forces conduct IO), information superiority (the object of IO), and the categories of IO (offensive IO and defensive IO). It also discusses how IO applies across the spectrum of conflict and its relationship to intelligence, surveillance, and reconnaissance. The chapter concludes with IO training considerations.

INFORMATION ENVIRONMENT

1-1. The *information environment* is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself (JP 3-13). It includes—

- The worldwide interconnection of communications networks.
- Command and control (C2) systems of friendly and adversary forces and other organizations.
- Friendly, adversary, and other personnel who make decisions and handle information.

Climate, terrain, and weapons effects (such as electromagnetic pulse or blackout) affect the information environment but are not part of it. Army forces increasingly rely on the unrestricted use of the information environment to conduct (plan, prepare, execute, and assess) full spectrum operations.

1-2. The information environment is one of the components of battlespace (see FM 3-0). A commander's area of interest now includes part of the information environment. The part of the information environment within a commander's battlespace encompasses information activities that affect an operation. To visualize it, commanders consider the dimensions of the entire information environment. They seek to understand how activity in the information environment may affect their mission. Commanders determine information activities that affect their operations and C2 systems, and those they can influence. Activities in the information environment that commanders cannot influence may force them to assume or act to mitigate risk.

1-3. The requirement for commanders to conduct reachback operations has expanded the portion of the information environment within a commander's area of interest. It now includes tactical to strategic C2 systems connected through the Global Information Grid (GIG). Commanders depend on support by elements of the GIG they do not control. They therefore rely on strategic defensive IO to ensure necessary connectivity.

1-4. Many significant actors in the information environment can affect the strategic, operational, and tactical direction of military operations—perhaps before they begin. Examples of these actors include—

- Foreign governments.

- US governmental agencies.
- Nongovernmental organizations.
- Agencies that coordinate international efforts.
- Social and cultural elements, and their leaders.
- Leaders of other Services, multinational partners, and adversaries.
- Individuals able to communicate with a worldwide audience.
- The news media.

1-5. All military operations take place within the information environment, much of which is largely outside the control of Army forces. Commanders consider the political and social implications that isolated small unit actions might produce. Within this context, commanders face many new challenges and opportunities. The complex relationship among political, strategic, technological, and military factors requires adopting a broad perspective of how operations and the information environment affect each other.

INFORMATION-ENVIRONMENT-BASED THREATS

1-6. Information-environment-based threats target one of three objects: commanders and other important decisionmakers, C2 systems, or information systems (INFOSYS). The Army defines a *command and control system* as the arrangement of personnel, information management, procedures, and equipment and facilities essential to the commander to conduct operations (FM 6-0). The Army defines *information systems* as the equipment and facilities that collect, process, store, display, and disseminate information. This includes computers—hardware and software—and communications, as well as policies and procedures for their use (FM 3-0). C2 systems contain INFOSYS. Preventing commanders from exercising effective C2 is the goal of adversaries operating in the information environment. They seek to achieve it by attacking C2 systems or the INFOSYS they contain.

1-7. Threats against friendly C2 systems vary across the spectrum of conflict (peace, crisis, and war) and by potential adversaries' technical capabilities and motivation (see FM 3-0). Threats have many sources and use many attack methods. Commanders and staffs evaluate them based on several criteria—some technical, some not. The following paragraphs discuss threat capabilities and sources, methods of attack, and evaluation criteria.

Threat Capabilities and Sources

1-8. Most threats to units engaged in offensive, defensive, and stability operations are straightforward and familiar. During these types of operations, commanders expect adversaries to conduct some form of IO against them and their C2 systems. They assume that adversaries will use multiple means to try to deny them information, cast doubts on information they have, and disrupt their decisionmaking process. However, the information environment contains other threats as well. These threats are worldwide, technically multifaceted, and growing. They come from a range of sources with varying capabilities—from individuals, to organizations, to nation-states. Military, political, social, cultural, ethnic, religious, or personal factors may motivate them. Commanders anticipate these threats, prepare defenses, and—when appropriate—conduct IO against them.

1-9. **Threat Capabilities**. The capabilities of adversaries operating in the information environment are ranked as follows:

- **First level**. Lone or small groups of amateurs using common hacker tools and techniques in an unsophisticated manner without significant support.
- **Second level**. Individuals or small groups supported by commercial business entities, criminal syndicates, or other transnational groups using common hacker tools in a sophisticated manner. This level of adversary includes terrorists and nongovernmental terrorist organizations. Their activities include espionage, data collection, network mapping or reconnaissance, and data theft.
- **Third level**. Individuals or small groups supported by state-sponsored institutions (military or civilian) and significant resources, using sophisticated tools. Their activities include espionage, data collection, network mapping or reconnaissance, and data theft.
- **Fourth level**. State-sponsored offensive IO, especially computer network attacks (CNAs), using state-of-the-art tools and covert techniques conducted in coordination with military operations.

1-10. Threat sources are listed at the right. Boundaries among these threats and among the capability levels are indistinct, and it is often difficult to discern the origins of any particular incident. For example, actions that appear to be the work of first level threat may actually be the work of a fourth level attack. In addition to active adversary actions, information fratricide can also threaten IO success.

Threat Sources

- Hackers
- Insiders
- Activist nonstate actors
- Terrorists
- Foreign IO activities
- Information fratricide

1-11. **Hackers**. Hackers are unauthorized users who attempt to or actually gain access to C2 systems and INFOSYS, or deny their use to legitimate users. They are often people who enjoy exploring the details of programmable systems and determining how to stretch their capabilities. The worldwide spread of INFOSYS in general, and the establishment of the Internet in particular, has led to a new threat: mass attacks by hackers to make political statements. This phenomenon is notable because it crosses national boundaries. When groups of activists believe that an entity is acting contrary to their goals, they make a global call for hackers to attack their perceived adversary. Calls to arms are made to individuals based on personal beliefs and morality; response to such a call is nearly impossible to predict. Even if hackers do not penetrate the target's C2 system, the number of attempts may have the effect of a denial of service attack.

1-12. **Insiders**. Insiders are individuals with legitimate access to elements of a C2 system. They pose one of the most serious threats to C2 systems. Whether recruited or self-motivated, insiders have access to INFOSYS normally protected against attack.

1-13. **Activist Nonstate Actors**. Nonstate actors, ranging from drug cartels to social activists, are taking advantage of the possibilities the information environment offers. They can acquire capabilities to strike at foes' C2

systems at low cost. Moreover, they can strike with relative impunity from a distance. Besides attacking opponents directly, these actors use the international news media to attempt to influence global public opinion and shape decisionmaker perceptions.

1-14. **Terrorists**. Terrorist actions range from gaining unauthorized access to C2 systems to physical attacks against commanders and decisionmakers. Terrorist groups have been identified as using commercial INFOSYS—especially computer bulletin boards—to pass intelligence and technical data across international borders.

1-15. **Foreign Information Operations Activities**. During peace, crisis, and war, foreign nations conduct IO against Army C2 systems, INFOSYS, and information. These actions will, in most cases, mimic those activities of hackers, terrorists, and activist including nonstate actors. Foreign IO activities take advantage of the anonymity offered by computer bulletin boards to hide organized collection or disruption activities. Some also masquerade as unorganized hackers. Their primary targets are often commercial and scientific, rather than military, INFOSYS. In addition, adversaries use IO capabilities—both low-tech and high-tech—to attempt to shape the information environment in their favor.

1-16. During crisis or war, adversary IO may attack commercial INFOSYS and military C2 systems on which Army forces rely. These attacks may take the form of jamming, broadcasting false signals and deceptive transmissions, or generating electromagnetic pulses. In such cases, adversaries can disrupt more than communications. Sensors at all levels can be jammed or triggered to produce misleading information. Commercial systems and sensors are particularly vulnerable to the effects of electromagnetic pulse due to their relatively unshielded architectures.

1-17. Foreign IO may actively seek to manipulate, knowingly or unknowingly, other threat sources. In particular, foreign intelligence services may use the threat of blackmail and other forms of trickery to cause other parties to act or facilitate actions on their behalf.

1-18. **Information Fratricide**. ***Information fratricide is* the result of employing information operations elements in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely affect friendly forces.** A familiar example is friendly force jamming degrading friendly radio communications. However, information fratricide covers other IO aspects as well. Actions, perceptions, and information from friendly forces that create improper impressions can adversely affect IO in sensitive situations. For example, working with an international organization that is locally controlled by a leader opposed to the US effort can give the wrong perception to the local populace.

1-19. Threat sources at all capability levels are present during peace and crises. Commanders consider their presence during war, even while focusing on the combined arms operations of the identified enemy. For example, the threat posed by insiders depends on their access to components of a C2 system. Likewise, a well-funded nonstate actor can pose a greater threat than some less sophisticated foreign intelligence services. Information fratricide also threatens IO success during peace and crisis. Effective staff work is

essential to ensure that the activities and messages of all forces and agencies are synchronized to achieve national objectives.

Methods of Attack

Methods of Attack
- Unauthorized access
- Malicious software
- Electromagnetic deception
- Electronic attack
- Physical destruction
- Perception management

1-20. Adversaries may use several methods to attack friendly C2 systems and INFOSYS, or shape the information environment in their favor. The nature of the information environment makes such attacks hard to detect. Some attacks, such as corrupting databases or controlling programs, can be designed with delayed effects. Others may employ immediate actions to degrade or destroy information nodes. Possible attacks are called incidents. An *incident* is an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users knowledge, instruction, or intent (JP 3-13).

1-21. **Unauthorized Access**. Unauthorized access is designed to gain information from, insert data into, modify data stored within, or delete data from C2 systems. Individuals can log on to military networks, such as local area networks, from the Internet. Firewalls (software that provides network security) exist to prevent this. However, if a firewall is penetrated, the C2 system is penetrated. Unauthorized access need not originate from the Internet and proceed through a firewall breach. A person with physical access to a terminal connected to a C2 system (an insider) can gain unauthorized access.

1-22. **Malicious Software**. Inserting malicious software causes a computer to operate in a manner other than that intended by its users. Malicious software includes computer viruses, logic bombs, and programs designed to bypass protective programs. Files downloaded from the Internet may contain viruses that disrupt software or corrupt databases.

1-23. **Electromagnetic Deception.** *Electromagnetic deception* is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby, degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are manipulative electromagnetic deception, simulative electromagnetic deception, and imitative electromagnetic deception (JP 3-51).

- *Manipulative electromagnetic deception* comprises actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces (JP 3-51). If not properly identified, manipulative electromagnetic deception may result in false information—signals, radiation, or data—being passed through the intelligence analysts, to the commander. Adversaries may pass inaccurate or

distorted information by indirect means (through the information environment) or direct means (such as deceiving friendly intelligence, surveillance and reconnaissance [ISR] systems).

- *Simulative electromagnetic deception* comprises actions to simulate friendly, notional, or actual capabilities to mislead hostile forces (JP 3-51). For example, a military deception operation may place surveillance radars in a typical defensive array when, in fact, the commander's intention is to attack.
- *Imitative electromagnetic deception* is the introduction of electromagnetic energy into enemy systems that imitates enemy emissions (JP 3-51).

1-24. **Electronic Attack**. *Electronic attack* is that division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Electronic attack includes (1) actions taken to prevent or reduce an adversary'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) (JP 3-51). Electronic attack (EA) against friendly C2 systems and their associated networks can occur at any time—during peace, crisis, or war. Army C2 systems are always subject to attack, regardless of the level of international tensions or hostilities.

1-25. Adversaries may try to inhibit operations by shutting down networks through electronic means. Some adversaries can conduct computer network attacks (CNAs) as well. Computer networks are particularly vulnerable to denial of service attacks. Networks do not have to be compromised or destroyed to disable them. Hackers can deny use of a network or other INFOSYS without gaining access to it. This capability makes denial of service attacks hard to defend against.

1-26. **Physical Destruction**. Weapons that can destroy, disrupt, or degrade C2 systems by physically destroying parts of them range from terrorist bombs to artillery, missiles, and aircraft. The ability of adversaries to strike will only grow as more capable systems, such as cruise missiles and precision-guided munitions, proliferate. The spread of such technologies as global positioning systems, unmanned aerial vehicles, and near real-time-imagery satellites, will enhance precision-strike capabilities.

1-27. **Perception Management**. *Perception management* consists of actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover, deception, and psychological operations (JP 3-13). Some adversaries will target friendly forces and interests with perception management activities, such as propaganda and deception, to

undermine their will to fight or resist. These activities can take many forms, from civilian media broadcasts to special operations forces strikes.

1-28. Propaganda seeks to shape the information environment in the adversary's favor. Strategic propaganda supports adversary strategic or operational objectives by influencing the opinions, emotions, attitudes, or behavior of people who can affect friendly operations. Operational and tactical propaganda seeks to incite opposition to friendly operations by targeting audiences in the area of operations (AO). Tactical propaganda may also attempt to influence the attitudes, emotions, motivations, and reasoning of commanders and members of friendly forces.

1-29. Deception is another means of shaping the information environment. However, it is usually targeted against a decisionmaker rather than a large population. Deception operations portray a false image of the situation. Their object is to lead friendly commanders to act in ways that favor the adversary. Common forms of deception include portraying false information about the exact strength and composition of adversary forces, their deployment and orientation, and their intended manner of employment. Military deception operations are deception operations conducted by Army forces (see chapter 4).

Evaluation of Information-Environment-Based Threats

1-30. Because the information environment contains more than just technical threats, commanders evaluate threats from several perspectives. Commanders and staffs consider the following factors:

- **The adversary C2 system**. Does the adversary C2 system include computers, networks, and other digital devices? Or, does the adversary use less technical ways to exercise C2?
- **Sources of information**. What is the best way to collect information from the adversary C2 system? The sophistication and technical complexity of the adversary C2 system determine the means required to exploit it.
- **Adversary goals and interests**. What are adversary short- and long-range goals? Can friendly forces affect them?
- **Influential groups, individuals, and decisionmakers**. What individuals or groups determine adversary or other group actions? These people may be leaders within the adversary armed forces or government, or interest groups in the information environment. They may be located within or outside the AO. Decisionmakers may be commanders or trusted subordinates.
- **Adversary IO resources and capabilities**. What resources can adversaries use to protect their C2 systems or inhibit friendly mission success? These may change over time. Adversaries may gain, lose, or reconstitute IO resources and capabilities, based combat actions or outside support. Accurately understanding current adversary capabilities is essential to success in a fast-moving operational environment.
- **Adversary IO vulnerabilities**. Where and how are adversaries vulnerable? How can friendly forces exploit those vulnerabilities? What are adversaries doing to keep friendly forces from exploiting them?

- **Friendly vulnerabilities to adversary IO efforts**. How is the friendly force vulnerable? What can it do to keep adversaries from exploiting those vulnerabilities?

INFORMATION ENVIRONMENT CHALLENGES

1-31. The complexity of the information environment presents commanders with significant and interrelated challenges. Most operations are conducted in full view of a global audience. Information technology changes rapidly, affecting friendly and adversary operations, and how they are perceived. Commanders face challenges in the areas of policy and public opinion, soldier morale, and legal considerations.

Policy and Public Opinion

1-32. The global expanse of the information environment allows news reports and analyses to rapidly influence public opinion and decisions concerning military operations. Audiences include the US public, decisionmakers, multinational partners, other nations, and international organizations. It also includes potential or actual adversaries. The news media will likely provide 24-hour coverage of, and diverse perspectives on, any future operation.

1-33. Global visibility of operations can also affect strategic or operational deterrence and affect commanders' decisions. Stories in the global information environment may be inaccurate, incomplete, or presented out of context. They may be based on rumor or be the result of intentional disinformation efforts. In such circumstances, commanders may be tempted to act in haste, make emotional decisions, or make choices inconsistent with the real situation. Effective commanders anticipate how adversaries might attempt to shape the information environment. Preventing adversaries from setting the terms of a conflict in the public arena is a form of maintaining the initiative and a fundamental aspect of perception management.

Morale

1-34. The global audience's perception of an operation may affect a command's combat power by influencing soldier morale. The rapid capabilities of modern communications systems often disseminate information—accurate or inaccurate—to soldiers faster than the chain of command does. Such activities as the will to win, dedication to the cause, understanding of the mission, and devotion to fellow soldiers and the unit can affect aspects of the human dimension (see FM 22-100). Because the human dimension includes families and communities as well as soldiers, a commander's battlespace includes home station (see FM 3-0). Bad news, misinterpretations, misinformation, and disinformation can affect morale there and indirectly undermine the will of the force.

Legal Considerations

1-35. Legal use or access to INFOSYS and technologies is rapidly changing as new laws and regulations are implemented. Even so, existing laws are often outdated. Commanders may face complex legal challenges and other constraints, such as, rules of engagement, treaties, or status of forces/mission agreements. Commanders include the staff judge advocate in the conduct of IO to ensure that legal and policy issues are thoroughly addressed.

INFORMATION SUPERIORITY

1-36. The Army defines *information superiority* as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (FM 3-0). This definition differs slightly from the joint definition. While joint doctrine considers information superiority a capability, Army doctrine establishes it as an operational advantage. For Army forces, information superiority describes the degree of dominance that commanders have over the part of the information environment that affects their operations, and over the adversary. Commanders measure it in terms of information-based activities. Gaining and maintaining information superiority creates conditions that allow commanders to shape the information environment and enhance the effects of other elements of combat power. Commanders direct three interdependent contributors to achieve this goal:

- Information management.
- Intelligence, surveillance, and reconnaissance.
- Information operations (including related activities).

INFORMATION MANAGEMENT CONTRIBUTIONS

1-37. *Information management* is the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decisionmaking. It uses procedures and information systems to collect, process, store, display, and disseminate information (FM 3-0). Information management (IM) consists of INFOSYS (see paragraph 1-6) and relevant information (RI). *Relevant information* is all information of importance to commanders and staffs in the exercise of command and control (FM 3-0). The G-6 exercises primary staff oversight for IM. The G-6 maintains the status of INFOSYS and ensures the C2 system provides relevant information to the commander and staff based on the priorities the commander establishes.

1-38. IM is integral to C2. Commanders drive IM by establishing commander's critical information requirements (CCIR). CCIR tell the staff which RI is most important to the commander. This RI is given priority for processing within the C2 system. FM 6-0 discusses the role of IM in C2, including providing support to achieving situational understanding, decisionmaking, and execution information.

1-39. An important IM enabler is network operations (NETOPS). NETOPS provide the collaborative, integrated management of networks, information systems, and resources that produce the common operational picture. NETOPS is performed from the strategic to the tactical extension of the GIG. It includes network management, information assurance, and information dissemination management. Effective NETOPS ensure that networks and INFOSYS are available, protected, and able to pass RI throughout the AO.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE CONTRIBUTIONS

1-40. The G-3 synchronizes intelligence, surveillance, and reconnaissance (ISR). ISR is an enabling operation that integrates and synchronizes all battlefield operating systems to collect RI to facilitate the commander's decisionmaking.

1-41. The G-2 has staff responsibility for producing intelligence about adversaries and the environment. Intelligence analysts process and analyze information (to include open-source information) to produce intelligence. They incorporate IO aspects into intelligence preparation of the battlefield (IPB) to develop an accurate description of adversaries, other individuals and groups, and the environment throughout the area of interest. Intelligence production focuses on answering priority intelligence requirements (PIRs) and identifying high-payoff targets.

1-42. *Priority intelligence requirements* are those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decisionmaking (FM 3-0). They are the subset of CCIR that deal with adversaries, other individuals and groups, and the environment. PIRs establish priorities for ISR. As part of the CCIR, they establish priorities for IM as well. PIRs tell soldiers, especially those performing ISR tasks, what to look for. PIRs tell soldiers in the C2 system which intelligence to disseminate first.

1-43. The G-7 contributes to the overall IPB by developing IO input for IPB (see chapter 5). The G-7 works with the G-2 to develop products that portray the information infrastructure of the AO and aspects of the information environment that can affect operations. In addition to information about adversary forces, these products include information on adversary and other decisionmakers, key people, and significant groups in the AO. They address potential strengths and vulnerabilities of adversaries and other groups as well as friendly force operations security (OPSEC) considerations.

1-44. Through the intelligence system, the G-2 has access to higher echelon information sources and ISR assets. Information from these sources is analyzed with information from organic sources to produce the adversary and environment portions of the operational picture (see FM 6-0). Advanced INFOSYS, adequate procedures, and trained soldiers allow the C2 system to disseminate this intelligence throughout the command. Effective IM provides different commanders and staffs with a common operational picture based on intelligence and friendly force information.

1-45. ISR provides input essential to IPB and the targeting process (see FM 34-130; FM 6-20-10). The three are interrelated. An accurate IPB requires effective ISR. Identifying, engaging, and evaluating effects on targets requires synchronizing both processes.

1-46. The G-3 exercises primary staff responsibility over reconnaissance operations. To answer PIRs, the G-3 tasks organic reconnaissance and surveillance assets. Together, the G-2 and G-3 exploit all available resources to answer the PIRs. The G-7 submits information requirements to the G-2. Information requirements that cannot be answered with organic assets are submitted to appropriate agencies as requests for information (RFIs).

INFORMATION OPERATIONS CONTRIBUTIONS

1-47. The IO concept brings together several previously separate functions as IO elements and related activities. Commanders use the IO elements/related activities to shape the information environment.

1-48. Successful IO depends on effective ISR and IM. ISR occurs both within and outside the C2 system. Surveillance and reconnaissance assets collect data throughout the area of interest. Intelligence assets process this data into intelligence. Commanders use this intelligence to focus the other elements of combat power. IM occurs within the C2 system. It enables both ISR and IO. Effective IM ensures intelligence and other RI gets to the commander in time to make decisions. Commanders apply the leadership element of combat power by using their judgment to make those decisions.

1-49. IM, IO, and ISR each have a different focus. ISR collects data and produces intelligence. IM disseminates and uses RI throughout the C2 system. IO applies that RI to protect the friendly C2 system, attack the adversary C2 system, and shape the information environment. All are essential to achieving and maintaining information superiority.

ACHIEVING INFORMATION SUPERIORITY

1-50. To achieve information superiority, commanders focus efforts to improve the friendly operational picture while affecting adversary battlefield perceptions in a way that leads them to make decisions favoring friendly forces. This situation provides a window of opportunity for decisive operations at times and places the commander chooses. Absolute and sustained information superiority is not possible. Adversary actions, friendly counteractions, and adversary reactions frequently determine how long friendly forces can exploit it.

1-51. Adversaries exercise a variety of means to protect their C2 systems. Some use means similar to those of friendly forces; others employ asymmetric means and methods. Similarly, adversaries use various capabilities to attack friendly C2 systems and shape the information environment in their favor. Regardless of friendly force capabilities, information superiority can decay quickly. A technologically equal opponent can use technological means to negate friendly information superiority. A technologically inferior opponent may use less sophisticated means or superior technology in one area to counter friendly capabilities. Thus, friendly commanders do not seek to sustain information superiority over an extended period. They act to forge localized information superiority when and where it produces decisive results.

1-52. Information superiority exists relative to an adversary. Commanders may not know when they have information superiority. However, when the information available to commanders allows them to accurately visualize the situation, anticipate events, and make appropriate, timely decisions better than adversary commanders can, information superiority exists. 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 its advantages and possibly wrest it from them. Commanders achieve information superiority by maintaining accurate situational understanding through effective IM (including NETOPS) and ISR while creating a disparity between reality and how adversaries perceive it. The more IO shapes this disparity, the greater the friendly advantage.

ASPECTS OF INFORMATION OPERATIONS

1-53. ***Information operations*** **is the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decisionmaking**. (This definition supersedes the definition of IO in FM 3-0. It is consistent with joint initiatives.) Commanders are flexible when determining how to exploit IO. The type of exploitation depends on their IO capabilities and objectives. As adversary C2 systems become more sophisticated, the friendly commander's decisionmaking window becomes smaller. Conversely, if adversary C2 systems are less sophisticated, the commander's ability to affect them directly with sophisticated capabilities becomes less likely. A friendly force with electronic warfare capabilities may dominate an opponent with a radio-based C2 system and no redundancy. However, an asymmetric environment may include an adversary with a C2 system based on courier/word of mouth capabilities that require Army forces to adopt equally unsophisticated IO methods. Countering the diverse threats in of the information environment demands imagination and creativity. The quick pace of IO places a heavy demand on preplanned IO branches and sequels (see FM 3-0).

1-54. Commanders from brigade through echelons above corps conduct IO. Responsibilities vary by echelon based on IO element and type of military operation.

ELEMENTS OF INFORMATION OPERATIONS

1-55. IO are enabling operations that create and present opportunities for decisive operations. Commanders use both offensive IO and defensive IO simultaneously to accomplish the mission, increase their force effectiveness, and protect their organizations and systems. IO elements include core capabilities and supporting capabilities (see figure 1-1, page 1-14). Commanders conduct IO through a combination of these elements and related activities. Figure 1-2, page 1-15, shows the relationship between the IO elements/ related activities, the types of operations, and unit responsibilities.

1-56. The elements of IO are not organizations. They are independent activities that, when taken together and synchronized, constitute IO. Commanders decide which IO elements are appropriate to accomplish the mission. All elements may not be required for each operation.

1-57. With the possible exceptions of computer network operations (CNO), CNA, computer network defense (CND) and computer network exploitation (CNE), no IO element is new. What is new is bringing these elements/related activities together as components of the information element of combat power. IO focuses efforts that before were diffuse. A single staff officer—the G-7—is assigned authority and responsibility for these previously separate activities. This allows commanders to mass the effects of the information element of combat power.

Core	Supporting
• Electronic warfare • Computer network operations • Computer network attack • Computer network defense • Computer network exploitation • Psychological operations • Operations security • Military deception	• Physical destruction • Information assurance • Physical security • Counterintelligence • Counterdeception • Counterpropaganda

Figure 1-1. Information Operation Elements

1-58. IO related activities include but are not limited to public affairs (PA) and CMO. Although FM 3-13 discusses only these two, any activity that contributes to gaining and maintaining information superiority (for example, an operation in support of diplomatic efforts conducted by special operations forces) may be considered an IO related activity.

ARMY-JOINT INFORMATION OPERATIONS RELATIONSHIPS

1-59. IO, by their nature, are joint operations. Each Service component contributes to an integrated whole synchronized by the joint force headquarters. All Army IO flow from the theater campaign plan. Army IO support joint force missions and receive support from joint force assets. Based on the unit mission, IO are integrated throughout the joint force to prevent information fratricide by different Services or different echelons (see JP 3-13; FM 3-0). In multinational operations, the US joint force commander (JFC) is responsible for coordinating the integration of US and multinational IO.

1-60. The IO cell at joint force headquarters deconflicts and synchronizes joint force IO. All Service components are represented. The joint force IO cell synchronizes all the Service-specific IO elements/related activities to achieve unity of effort supporting the joint force. Army forces submit requests for IO support from joint force or higher echelons through the senior Army headquarters to the joint force IO cell.

OFFENSIVE INFORMATION OPERATIONS

1-61. The Army defines *offensive information operations* as the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decisionmakers or to influence others to achieve or promote specific objectives (FM 3-0). The Army definition deletes a sentence in the joint definition that lists IO elements associated with offensive IO. Army doctrine allows commanders to use all IO elements offensively.

Type of Operation	Offensive & Defensive				Stability				Support			
IO Element/Related Activity	**ASCC**	**Corps**	**Div**	**Bde**	**ASCC**	**Corps**	**Div**	**Bde**	**ASCC**	**Corps**	**Div**	**Bde**
OPSEC	P E	P E	P E	P E 4	P E	P E	P E	P E 4	P E	P E	P E	P E 4
PSYOP	P E	P E A	P E A	P 1, 2/ E A 4	P E	P E A	P E A	P 1, 2/ E A 4	P E	P E A	P E A	P 1, 2/ E A 4
Military Deception	P E	P E	P E A	P E 4	PE	P E	P E	E 4	X	X	X	X
EW–EA	P E	P E	P E	E A 4	P E	P E	P E	E A 4	X	X	X	X
EW–ES	P E	P E	P E	P E 4	P E	P E	P E	E 4	P E	E	E	E 4
EW–EP	P E	P E	P E	P E 4	P E	P E	P E	P E 4	P E	P E	P E	P E 4
CNO	P	P	X	X	P	X	X	X	X	X	X	X
CNA	P	P	X	X	P	X	X	X	X	X	X	X
CND	P E	P E	P E	P E 4	P E	P E	P E	E 4	P E	P E	P E	E 4
CNE	P	P	X	X	P	X	X	X	X	X	X	X
Physical Destruction	P	P E	P E	P E 4	P	P E	P E	P E 4	X	X	X	X
IA	P E	P E	P E	P E 4	P E	P E	P E	P E 4	P E	P E	P E	P E 4
Physical Security	P E	P E	P E	P E 4	P E	P E	P E	P E 4	P E	P E	P E	P E 4
Counterintelligence	P E	P E	P E	P E A 1 2	P E	P E	P E	E A 4	P E	P E	P E	E A 4
Counterdeception	P E	P E	P E	P E 1 2	P E	P E	E	E 4	P E	P E	E	E 4
Counterpropaganda	P E	P E	P E	P E 4	P E	P E	P E	E 4	P E	P E	E	EA 4
Related Activity												
CMO	P E	P E	P E	P E A 4	P E	P E	P E	P E A 4	P E	P E	P E	P E A
Public Affairs	P E	P E	P E	E A 4	P E	P E	P E	E A 4	P E	P E	P E	E A 4

P – Plan/prepare element, objectives, and tasks as stated in OPLAN/OPORD
E – Execute the objective and task as stated in OPLAN/OPORD
X – Command is not involved with this element
A – Accomplished with attached assets

1 – Stryker brigade combat teams (SBCT)
2 – Enhanced Army National Guard brigades
3 – Divisional maneuver brigades
4 – All brigades

Figure 1-2. Information Operations Responsibilities by Echelon

1-62. Commanders conduct offensive IO across the range of military operations and throughout the spectrum of conflict. The rules of engagement affect the means used and the effects sought in any given situation. Offensive IO facilitates seizing and retaining the initiative by creating a disparity between the quality of information available to friendly forces and that available to adversaries. The following effects create this information advantage:

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

to support friendly force missions or not resist friendly force activities. Perception management achieves the influence effect by conveying or denying selected information to targets.

DEFENSIVE INFORMATION OPERATIONS

1-63. The Army defines *defensive information operations* as the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes (FM 3-0). The Army definition deletes a sentence in the joint definition that lists IO elements associated with defensive IO. Army doctrine allows commanders to use all IO elements defensively.

1-64. Defensive IO seeks to limit the vulnerability of C2 systems to adversary action and to prevent enemy interference with friendly information and INFOSYS. Defensive IO effects include: protection, detection, restoration, and response.

1-65. **Protection. *Protection* is all actions taken to guard against espionage or capture of sensitive equipment and information**. In IO, protection occurs at the digital perimeter to control access to or mitigate the effects of adversary access to friendly decisionmakers and INFOSYS. Protection applies to both the quantity and quality of information. It denies the adversary information about friendly capabilities and intentions by controlling indicators.

1-66. **Detection. *Detection* is to discover or discern the existence, presence, or fact of an intrusion into information systems**. Detection is the identification of adversary attempts to gain access to friendly information and INFOSYS. Detection begins with INFOSYS users and administrators. Timely detection and reporting are the keys to initiating restoration and response. Electronic detection occurs at the internal digital perimeter.

1-67. **Restoration. *Restoration* is to bring information systems back to their original state**. Restoration is reestablishment of essential capabilities of INFOSYS damaged by enemy offensive IO. Restoration may rely on backup or redundant links, INFOSYS components, or alternative means of information transfer.

1-68. **Response. *Response* in information operations is to react quickly to an adversary's information operations attack or intrusion**. Timely identification of adversaries, their intent and capabilities, is the cornerstone of effective response to adversary offensive IO.

1-69. Defensive IO uses technical and nontechnical activities to limit the vulnerability of friendly C2 systems to hostile IO. It also seeks to prevent adversaries from tampering with friendly force information or interfering with friendly C2 systems. Defensive IO supports efforts to maintain effective C2 by countering or turning to friendly advantage adversary IO efforts. Timely, accurate intelligence—some of which is based on information collected during offensive IO—is essential to defensive IO. Forces conducting defensive IO

require information about adversary attack methods, tools, capabilities, weapons, and means of operation—which ISR produces.

RELATIONSHIP OF OFFENSIVE AND DEFENSIVE INFORMATION OPERATIONS

1-70. Commanders synchronize offensive and defensive IO to produce complementary and reinforcing effects (see FM 3-0). Offensive IO supports the decisive operation, while defensive IO protects friendly force critical assets and centers of gravity. Conducting offensive and defensive IO independently detracts from the efficient employment of IO elements. At best, it expends more resources than would be required if the two were done in concert. At worst, uncoordinated efforts increase conflicts and mutual interference. In the extreme, they may compromise friendly intentions or result in information fratricide. Fully integrating offensive and defensive IO requires planners to treat IO as a single function. Commanders assisted by their G-7s integrate offensive and defensive IO to gain and maintain information superiority. Commanders avoid concentrating on offensive IO to the exclusion of defensive IO. They employ all IO elements offensively and defensively. Often offensive and defensive IO use the same tactics, techniques, and procedures (TTP). The commander's intent and desired effects determine whether an information operation is offensive or defensive.

1-71. Commanders integrate offensive and defensive IO at all levels of war (see FM 3-0). At the strategic level, IO seek to engage adversary or potential adversary leadership to deter crises or end hostilities. At the operational level, IO focuses on denying adversaries the ability to conduct operations. Military deception may be the significant offensive IO element. At the tactical level, IO focuses on an adversary's use of information and INFOSYS. Lethal and nonlethal fires may be a significant contributor in offensive and defensive operations. PSYOP and CMO may be significant contributors in support operations and stability operations.

1-72. Tactical-level IO contributes to achieving strategic and operational objectives. Operational- and strategic-level IO facilitate tactical operations. Commanders also conduct IO across the range of military operations (see FM 3-0). IO can be a potent force multiplier during offensive, defensive, and support operations, and may be the decisive operation during stability operations.

1-73. The complexities and scope of the information environment make it difficult to achieve the desired effects with a single IO element. Effective integration and synchronization of all IO elements is necessary to achieve mutual support. Likewise, protecting friendly C2 systems and their components requires careful integration and synchronization of IO elements. Two ways of integrating are deconflicting and coordinating.

1-74. Commanders synchronize IO to cause specific effects at decisive points to support the overall operation. Synchronizing offensive and defensive IO is more effective than conducting them independently. Activities of all IO elements often occur simultaneously. Synchronizing them results in complementary and reinforcing effects. It also decreases the probability of conflicts and interference that may compromise friendly intentions or result in information fratricide.

INFORMATION OPERATIONS ACROSS THE SPECTRUM OF CONFLICT

1-75. The national security and national military strategies establish an imperative for engagement (see FM 1). Engagement involves the nation exercising the instruments of national power—diplomatic, informational, military, and economic—to shape the security environment. One means by which the United States exercises the informational instrument of national power is through joint IO. Army forces conduct IO within joint force parameters. Throughout the spectrum of conflict, commanders conduct IO to apply the information element of combat power. In all situations, Army forces do not act in isolation. Almost all operations are joint; most are interagency as well.

PEACE

1-76. During peace, commanders conduct IO to shape the strategic environment or to prepare for operations during crisis and war. Normally IO are part of a combatant commander's theater engagement plan. The majority of peacetime preparation is done at home station or during training exercises. Using contingency plans to focus their efforts, commanders prepare databases for each IO element. These databases contain information on possible adversaries and other significant actors. At the strategic and operational levels, databases focus on one or more of the following target sets:

- Political leadership.
- Information capabilities and vulnerabilities, including military and civilian communication networks, and domestic and foreign media.
- Military operations, leadership, and infrastructure, and their vulnerabilities at the strategic, operational, and tactical levels.
- Economic factors that affect an actor's ability to mount and sustain military operations, and those that affect the morale of the population and its leadership. This set includes the infrastructure that supports economic activity.
- Social effects of ethnic, racial, and historical animosities and alliances.

1-77. The first four of these target sets coincide with the instruments of national power. The last target set addresses aspects of the information environment that commanders consider when conducting IO. Examples of information that databases may include are—

- People and groups who wield influence, both within states and nonstate actors.
- Decisionmakers, both within states and nonstate actors.
- People and groups sympathetic to US interests.
- People and groups hostile to US interests.
- People and groups vulnerable to US influence.
- Themes that appeal to specific audiences.
- Attributes of states that make them stable or unstable.
- States and nonstate actors that either accept or reject US economic or military support.
- Religious, ethnic, and cultural customs, norms, and values.

- Assessments of communications infrastructure.
- Assessments of military communication and C2 infrastructures.
- Assessments of military training and proficiency (to determine susceptibility to denial, military deception, and psychological operations).
- Literacy rates.
- Assessments of ethnic factional relationships and languages.

1-78. During peace, execution of some IO activities requires strategic-level approval (see figure 1-2, page 1-15). However, IO assessment, planning, preparation, and training during peace allow commanders to develop links between governmental and nongovernmental agencies that are useful during crisis and war. These activities also allow different echelons to coordinate and deconflict their IO plans before receiving a mission. Commanders at all echelons can determine the approval authority for the various IO elements/related activities and synchronize their plans. Commanders also learn to recognize the risks involved and the tradeoffs required to conduct effective IO.

1-79. Department of Defense (DOD) and other intelligence agencies publish reports and other products to support contingency planning (see AR 381-11). These are available under the DOD Intelligence Dissemination Program. New production requirements, less requirements for signals intelligence end products (SEPs), are processed under the Department of Defense Intelligence Production Program. Authorized users submit requests using the automated Community On-line Intelligence System for End Users and Management (COLISEUM). SEP requirements are submitted through major Army commands to the United States Army Intelligence and Security Command (INSCOM).

1-80. In addition to preparing for possible contingencies, some forces conduct IO to accomplish the objectives of an actual deployment. For example, IO has been a major, if not the decisive, aspect of peace operations in the Balkans. Commanders conduct IO to influence decisionmakers and other actors in the information environment. During peace, IO are often the primary means geographic combatant commanders use to shape the strategic environment.

CRISIS

1-81. During crises, Army forces conduct IO based on existing contingency plans or a crisis action plan (see JP 5-0). A potential or actual contingency requires commanders at all echelons to gather additional information and refine their contingency plans based on a specific AO or target set. Geographic combatant commanders may use the relationships and conditions in the information environment created during peace to influence potential adversary decisionmakers to act in ways that will resolve the crisis peacefully. Other IO may attempt to influence actors within the target group's political, economic, military, and social structures. Still other IO collect information about target groups to use in decisionmaking and in conducting operations, if necessary. Operational and tactical commanders prepare for IO as part of their deployment preparations. They coordinate preparations with the JFC to ensure unity of effort and prevent information fratricide. Preparing for IO includes obtaining information about potential adversaries from all available sources.

1-82. Information in the social and informational target sets shape commanders' thinking about the AO. The military target set focuses operational planning and preparation. Commanders conduct IO to develop the situation and refine their situational understanding. Some IO elements/related activities are more suited for this than others. For example, PA shape the information environment by keeping the US public informed. Counterdeception may reveal adversary intentions. Counterpropaganda may be able to stabilize a crisis. CND can ensure that timely and accurate information is transmitted within the command so a common operational picture is available for decisionmakers (see FM 6-0). The objective during a crisis is to move the potential conflict back towards peace. The more subtle IO elements can help accomplish this.

1-83. During crises, commanders may be authorized to conduct more focused ISR operations against possible adversaries to prepare for operations. This means devoting additional resources to the collection effort (offensive IO). Effective contingency planning helps commanders determine what information requirements must be met to execute an operation. Commanders obtain approval for IO tasks and products developed during contingency planning and preparation. They also execute operations with objectives that require a long time to achieve. As figure 1-3, page 1-22, shows, IO elements have different approval chains, and many IO activities may require a long time to approve.

WAR

1-84. During war, commanders conduct IO to synchronize the information element of combat power with the other elements of combat power. Well-synchronized offensive IO can cripple not only adversary military power but also adversary civilian decisionmaking capability. Commanders and staffs follow the military decisionmaking process to plan IO that accomplishes the commander's intent and concept of operations. Part Two describes how they do this. Appendix B provides an example scenario.

THE G-7 SECTION AND THE INFORMATION OPERATIONS CELL

1-85. The G-7 has coordinating staff responsibility for IO. He does this by means of the G-7 section and IO cell. The G-7 section has assigned officers and NCOs responsible for IO current operations, IO planning and IO targeting (see appendix F). The G-7 coordinates IO related activities of other staff officers through the IO cell.

1-86. The IO cell, located in the main command post, brings together representatives of organizations responsible for all IO elements and related activities. Related activities include any organizations able to contribute to achieving IO objectives. PA and CMO are always related activities; commanders may designate others. The IO cell also includes representatives of special and coordinating staff sections, as the mission requires. All battlefield operating systems are represented. The primary function of an IO cell is to synchronize IO throughout the operations process. In corps and divisions, the G-7 section forms its nucleus. In Army service component commands (ASCCs), the plans, current operations, and effects control divisions—under the deputy chief of staff for operations—coordinate IO. The ASCC ensures Army IO

supports the theater IO campaign plan. If another headquarters is designated as the ARFOR, that headquarters assumes this responsibility.

IO Element/Related Activity	IO Concept of Support	IO Objectives	IO Tasks
OPSEC	Planning headquarters	Planning headquarters	Planning headquarters
PSYOP	Planning headquarters	Joint force commander	Geographic combatant commander
Military Deception	Planning headquarters	Next higher headquarters	Next higher headquarters
Electronic Warfare	Planning headquarters	Planning headquarters	Planning headquarters
CNO	Planning headquarters	Planning headquarters	INSCOM & geographic combatant commander*
CNA	Planning headquarters	Planning headquarters	INSCOM & geographic combatant commander*
CND	Planning headquarters	Planning headquarters	NETCOM
CNE	Planning headquarters	Planning headquarters	INSCOM & geographic combatant commander*
Physical Destruction	Executing headquarters	Executing headquarters	Executing headquarters
Information Assurance	Planning headquarters	Planning headquarters	Executing headquarters
Physical Security	Planning headquarters	Planning headquarters	Planning headquarters
Counterintelligence	Planning headquarters	Echelon dependant	Task dependant
Counterdeception	Planning headquarters	Next higher headquarters	Next higher headquarters
Counterpropaganda	Planning headquarters	Joint force commander	Geographic combatant commander
*Approval for execution is with the Secretary of Defense			

Figure 1-3. Information Operations Approval Authorities

1-87. IO cell members may coordinate during meetings or over a local area network. The frequency and times of IO cell meetings are synchronized with the command's battle rhythm (see figure E-2, page E-3). The IO cell also identifies IO targets, which the G-7 nominates during targeting team meetings. IO cell members coordinate IO objectives and tasks with their counterparts at the higher and lower echelons. This coordination ensures that IO objectives and tasks at all echelons are synchronized.

TRAINING FOR INFORMATION OPERATIONS

1-88. Effective IO requires soldiers who have trained as they intend to fight. When commanders and units exercise IO elements realistically in training, the readiness and confidence of the force increases. Part Two contains TTP for IO. They form the basis for individual and collective IO training. When developing IO for exercises, the following considerations are important:

- Include IO in training objectives.
- Establish how achieving information superiority aids mission accomplishment.

- Develop concrete, attainable IO training objectives.
- Support exercise objectives with realistic play by all IO elements/related activities.
- Create a realistic IO exercise environment.
- Assess and evaluate employment and synchronization of IO elements/ related activities.
- Use appropriate security measures to protect IO activities.
- Evaluate the use of computer support products (such as synchronization tools) to execute IO.
- Use simulations to augment IO where and when applicable.
- Give credit to the playing units for IO execution; penalize those who should and do not.
- Apply effects of friendly offensive and defensive IO to opposing forces, and effects of adversary offensive and defensive IO to friendly forces.
- Require units to maintain mission effectiveness when they lose the support of digital/advanced technology.

1-89. Effective IO training requires products that contain specific information on adversary social, military, religious, and economic institutions. Exercise planners may have to provide these. The data needed to create, update, and use these products should be built into the exercise scenario and master scenario events list (MSEL). The opposing force should have an IO capability consistent with the exercise scenario. Realistic IO are essential to evaluating friendly IO proficiency. Within the exercise tenets, both sides should be allowed free IO play. Structured, mechanical IO degrades participants' ability to develop the mental agility and creativity that actual IO demand. Senior exercise participants should allow, even welcome, opportunities to work through the C2 chaos that effective IO can cause. Units should include IO tasks in their mission essential task lists (METLs).

SUMMARY

1-90. Information superiority is an operational advantage commander's gain through effective IM, ISR, and IO. Commanders from brigade through echelons above corps conduct IO to attack adversary C2 systems, defend friendly C2 systems, and shape the information environment. They conduct IO throughout the spectrum of conflict and across the range of military operations. IO brings together many elements and related activities. The G-7 has coordinating staff responsibility for IO. IO applies the information element of combat power. Properly synchronized, it enhances employment of the other elements of combat power. Successful IO helps commanders gain, maintain, and exploit the initiative. Available technology allows commanders to synchronize offensive and defensive IO to produce complementary and reinforcing effects. However, despite advances in technology, the human dimension remains the primary focus of IO.

Chapter 2

Information Operations Elements and Related Activities

This chapter discusses the contributions and links of each information operations (IO) core and supporting element and related activity to offensive and defensive IO. It also shows the links among them in diagram form. The core and supporting IO elements are similar to the battlefield operating systems. They are independent activities that, when taken together and synchronized, constitute IO. Figure 2-1, pages 2-27–2-30, shows how each IO element supports the others. Figure 2-2, pages 2-31–2-32, shows possible conflicts among IO elements. Figure 2-3, page 2-33, shows the support between IO and the related activities of public affairs and civil-military operations.

CORE ELEMENTS

2-1. Core IO elements are operations security (OPSEC), psychological operations (PSYOP), military deception (MD), electronic warfare (EW) and computer network operations (CNO). ***Computer network operations*** **comprise computer network attack (CNA), computer network defense (CND), and related computer network exploitation (CNE) enabling operations.** (This definition is consistent with joint initiatives and is being staffed as a possible joint definition). These core IO elements can be employed either individually or in conjunction with various supporting elements, related activities, and intelligence capabilities to provide a fully integrated warfighting capability.

2-2. PSYOP, MD and OPSEC are employed to influence adversary decisionmakers or groups while protecting friendly decisionmaking. EW and CNO are employed to affect or defend the electromagnetic spectrum, information systems (INFOSYS), and information that support decisionmakers, weapon systems, command and control (C2), and automated responses.

CONTENTS

OPERATIONS SECURITY

2-3. The Army defines ***operations security*** **as a process of identifying essential elements of friendly information and subsequently analyzing friendly actions attendant to military operations and other activities to—**

- **Identify those actions that can be observed by adversary intelligence systems.**
- **Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive essential elements of friendly information time to be useful to adversaries.**
- **Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation**.

The Army substitutes *essential elements of friendly information* (EEFI) for the joint term *critical information* in the joint definition of OPSEC. Otherwise, the two definitions are identical. The Army does not use the term *critical information.* The Army and joint definitions describe identical processes with the same objective: protect information that can impede or prevent the force from accomplishing the mission.

2-4. JP 3-54 establishes joint OPSEC doctrine. Chapter 3 establishes Army OPSEC doctrine. Duties of the OPSEC officer, a special staff officer, are listed in appendix F. OPSEC includes camouflage, concealment, and decoy employment. FM 20-3 discusses how camouflage, concealment, and decoy employment supports defensive IO in the Army and joint environments. FM 20-3 also discusses camouflage tactics, techniques, and procedures (TTP).

Contributions

2-5. OPSEC contributes to offensive and defensive IO. OPSEC is offensive when the desired effect is to deny adversaries information about friendly force actions, intentions, and future operations. It contributes to offensive IO by slowing the adversary decision cycle and directly affecting the quality of the adversary commander's decisions. OPSEC is defensive when the desired effect is to deny adversaries information that could be used for targeting or attacking friendly forces. Effective OPSEC measures based on solid planning starve the adversary intelligence system by denying it the information needed to produce intelligence.

Staff Coordination

2-6. Commanders establish routine OPSEC measures in unit standing operating procedures (SOPs). The OPSEC officer coordinates additional OPSEC measures with G-2, G-3 and other staff and command elements as necessary. The OPSEC officer develops OPSEC measures during the military decisionmaking process (MDMP) (see chapter 3). The G-2 assists the OPSEC process by comparing friendly OPSEC indicators with the adversary's intelligence collection capabilities. OPSEC measures are published in the OPSEC appendix to the IO annex to plans and orders. The G-7 exercises coordinating staff responsibility over the OPSEC officer.

PSYCHOLOGICAL OPERATIONS

2-7. *Psychological operations* are planned operations that convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately to influence the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives (JP 3-53). Only Department of Defense agencies (including Army forces) conduct PSYOP.

2-8. Strategic-level PSYOP are synchronized with International Public Information Program (IPIP). The IPIP coordinates dissemination of information about US foreign policy outside the United States, its territories, and its possessions through by various government agencies. Presidential Decision Directive 68 requires that information distributed through the IPIP not be designed "to mislead foreign audiences," and that information programs "must be truthful."

Contributions

2-9. Psychological operations can articulate to appropriate foreign audiences the mission, intent, and combat power of the force. It can also curb unreasonable expectations about the US role and actions during operations. PSYOP are a mainstay of US government efforts to influence foreign audiences at the strategic, operational, and tactical levels (see JP 3-53; FM 33-1-1).

2-10. PSYOP is a force multiplier. Its capabilities include—

- Increasing the effects of MD.
- Reinforcing adversary perceptions that support friendly operations.
- Planting doubts about the adversary leadership.
- Enhancing live-fire capability demonstrations with surrender appeals.
- Projecting the image of US superiority.
- Influencing foreign populations by expressing information in a fashion that affects attitudes and behavior.
- Obtaining compliance or noninterference with Army force operations.
- Facilitating operations; minimizing needless loss of life and collateral damage, and furthering objectives of the United States and its partners.

PSYOP personnel can also assist commanders by advising them of whom to influence and how.

2-11. Specific PSYOP techniques include—

- Identifying adversary information-gathering capabilities and actions.
- Ascertaining information and indicators that should be conveyed and denied to adversaries to reinforce desired perceptions and preserve essential secrecy.
- Developing themes and actions to be stressed or avoided to support attaining specific IO objectives.
- Using face-to-face communications, essential communicators, and mass media to channel adversary behavior.

2-12. PSYOP can also convince adversaries not to do something by describing results of their taking an undesired action. This type of operation is usually

conducted at the strategic level, but all PSYOP units reinforce the strategic message. Operational-level PSYOP, employed with other IO elements, seek to convince adversary decisionmakers that taking certain actions is in their best interest. PSYOP personnel integrate PSYOP actions, PSYOP enabling actions, and targeting restrictions into the targeting process. These actions and restrictions facilitate mission accomplishment, minimize adverse effects, and attack the adversary's will to continue. The actions may be based on political, cultural, ethnic, and religious considerations. They may also have historical, economic, military, or ideological origins. Regional, national, demographic, or geographic factors are also taken into account.

2-13. As with offensive IO, PSYOP transmit information that may degrade the morale and effectiveness of adversary commanders and units. As defensive IO, PSYOP can be used to deny adversary exploitation of the target population. PSYOP missions include—

- Projecting a favorable image of US actions by informing friendly, neutral, and hostile audiences in both denied areas and friendly areas.
- Bypassing censorship, illiteracy, or interrupted communications systems to convey messages to target audiences.
- Targeting adversaries to—
  - Degrade their morale.
  - Reduce their will to resist.
  - Discourage them from employing certain kinds of weapons, such as weapons of mass destruction (WMD).
  - Offer alternatives to continued conflict.
- Sustaining the morale of resistance fighters.
- Exploiting ethnic, cultural, religious, or economic differences.
- Influencing local support for insurgents.
- Providing intelligence regarding nonmilitary factors for contingencies.
- Disseminating rules of interaction and cultural information to US forces under the auspices of the unit internal information program.

2-14. Considerations during PSYOP planning include—

- **Legal constraints**.
  - PSYOP is prohibited from targeting audiences within the United States, its territories, or its possessions.
  - PSYOP must follow international law, treaties, and US law, especially when conducted offensively.
  - For additional details, see the Smith-Mundt Act of 1948; Presidential Decision Directive 68.
- **Approval authority**. PSYOP product approval authority can be no lower than the commander, joint task force (CJTF). There are two levels of PSYOP product approval:
  - **Objectives, themes, and messages**. The President, combatant commander, JFC, or appropriate ambassador approves objectives, themes, and messages.
  - **Products**. Commanders subordinate to CJTFs may modify approved products within guidelines issued by the higher headquarters to better target local audiences.

- **Influencing adversaries**. Commanders must be able to back up messages intended to influence adversaries with the truth.
- **Counterpropaganda**. One PSYOP unit responsibility is to conduct counterpropaganda programs. Counterpropaganda is discussed as a separate IO element.
- **Time constraints**. Some PSYOP effects require more time to achieve than others. For example, changing the mind-set of adversary decisionmakers takes longer than influencing an adversary to commit forces in response to a deception story. In addition, assessing the effects of PSYOP designed to produce intangible results generally requires more time than assessing those designed to produce tangible results.
- **Accessibility of potential target audiences**. The target audience may be beyond the limits of military PSYOP targeting methods due to physical or policy restrictions. Conversely, commanders must ensure their PSYOP effects are limited to their area of operations (AO). PSYOP that may cause effects beyond the AO are coordinated with the affected units or higher headquarters.
- **Logistic requirements for PSYOP**. Print and multi media requirements must be taken into consideration. Producing PSYOP products may increase requirements for paper, ink, magnetic media, and other printing supplies.

2-15. The following are examples of how strategic, operational, and tactical PSYOP forces can support both national and in-theater objectives. Commanders conduct PSYOP concurrently at strategic, operational, and tactical levels.

- **Strategic**. Strategic PSYOP use radio, television, and various forms of printed products. They can influence adversary civil populations to—
  - Deny or lessen support for their government.
  - Move (usually not the desirable action) or stay in place.
  - Actively oppose their government's actions.
- **Operational**. Operational PSYOP uses radio, television, and various forms of printed products. They can influence adversary civil populations to—
  - Stimulate support of opposition elements within the adversary force.
  - Support resistance activities.
  - Encourage disaffection of adversary.
- **Tactical.** Tactical PSYOP seeks to influence PSYOP targets directly. It uses face-to-face, limited production printed products and loudspeakers. Tactical PSYOP can—
  - Influence adversary civil populations not to interfere with friendly force efforts.
  - Induce cooperation or reduce active opposition.
  - Reduce collateral damage by giving instructions to noncombatants in the combat zone.

2-16. Both strategic and tactical PSYOP forces can increase the cooperation of civil authorities and populace with friendly forces. Some examples are—

- PSYOP can increase the safety of the populace by informing them of hazards such as mines and contaminated areas.
- PSYOP can assist in military traffic control and make public health announcements.
- A combination of civil-military operations (CMO), PSYOP, and public affairs (PA) operations can reduce the resources required to manage the AO and reduce the US-only force protection requirements.

Staff Coordination

2-17. With the G-2, G-3, and G-5, the G-7 evaluates enemy PSYOP efforts and the effectiveness of friendly PSYOP on target groups. Once PSYOP tasks are determined, the PSYOP officer coordinates them with higher headquarters for the G-7. The geographic combatant commander approves PSYOP tasks. A statement of requirements is a significant portion of the logistic and operational staff planning process in support of PSYOP (see FM 3-05.30). Duties of the PSYOP officer, a special staff officer, are listed in appendix F. The G-7 exercises coordinating staff responsibility over the PSYOP officer.

MILITARY DECEPTION

2-18. *Military deception* comprises actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (JP 3-58). (The complete joint definition includes definitions of five MD categories; see chapter 4.) It is used to make an adversary more vulnerable to the effects of friendly force weapons, maneuver, and operations. JP 3-58 contains joint doctrine for MD. Chapter 4 contains Army doctrine for MD. Duties of the military deception officer (MDO), a special staff officer, are listed in appendix F.

Contributions

2-19. MD operations deceive adversaries by manipulation, distortion, or falsification of evidence, and induce them to react in a manner prejudicial to their interests. Two ways of manipulating adversary commanders are—

- Increasing their uncertainty concerning friendly force intent.
- Reducing their uncertainty concerning a friendly course of action.

2-20. MD used offensively causes adversary commanders to act based on inaccurate impressions. Adversary actions may include wasting intelligence assets or failing to use other resources to their best advantage. MD used defensively hides friendly force capabilities and intentions.

Staff Coordination

2-21. The G-7 exercises coordinating staff responsibility over the MDO. This responsibility includes integrating MD into all operational planning. MD plans are normally prepared by a deception working group formed by the MDO. Psychological, MD, and OPSEC operations all deal with presenting or denying friendly force information to adversaries; they are interrelated and require detailed synchronization. In addition, MD and PSYOP often require

a long time to achieve effects. The approval of MD tasks is at the higher headquarters of the echelon assigned the task. The MDO—

- Coordinates with the G-2 to determine requirements or opportunities for MD operations.
- Coordinates with the G-3 and the G-7 to ensure the MD supports the commander's intent and concept of the operation.
- Recommends the deception target, deception objective, and deception story.
- Coordinates MD operations within the staff on a need-to-know basis.

2-22. Although the transparency required for traditional peacekeeping may preclude using MD, MD may be appropriate and necessary during peace enforcement operations. However, PSYOP may complicate the conduct of MD operations. PA can withhold information that could negate MD. The multinational and interagency character of peace enforcement operations may also complicate the MD effort, as it could confuse multinational partners if they not aware of it. Foreign area officers, multinational and special operations force liaison officers, and State Department personnel should be consulted during planning to ensure the messages sent to potential adversaries are appropriate.

ELECTRONIC WARFARE

2-23. *Electronic warfare* is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-51). (See JP 3-51 and FM 34-40 for detailed discussions of EW.)

Contributions

2-24. The three major components of EW are electronic protection (EP), electronic warfare support (ES), and electronic attack (EA).

2-25. **Electronic Protection**. *Electronic protection* is that division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability (JP 3-51). Friendly forces use emission control and other antijamming measures to perform EP.

2-26. **Electronic Warfare Support**. *Electronic warfare support* is that division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, ES provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signal intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence (JP 3-51). ES supports both offensive and defensive IO. It identifies, locates, and exploits adversary emitters (signals). It helps commanders achieve situational understanding and assess damage. It protects the force by producing

detailed information on adversary INFOSYS. Information produced by ES operations supports ISR operations. It gathers technical information that supports the development and maintenance of the electronic order of battle database used for EA and other ES operations.

Electronic Warfare in Peace Operations

EW capabilities that can support peace operations include jamming and sensor systems. In 1997, US forces in Bosnia used jamming and other military action to stop an anti-NATO propaganda campaign on Bosnian Serb television. Early in the mission, sensors were used to provide warning of military activity by indigenous paramilitary groups, assess their intentions, and determine their resolve to use military force. As the situation stabilized, EW operations shifted to monitoring indigenous paramilitary C2 systems for compliance with the military provisions of the Dayton peace accords. In addition, surveillance assets were used to monitor civilian and paramilitary movements.

2-27. **Electronic Attack**. *Electronic attack* is that division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Electronic attack 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) (JP 3-51). EA deceives adversaries, denies them information, and disrupts their C2 systems. There are trade-offs when jamming enemy C2 systems. Jamming may cause the loss of a collection source for a time. The source may change frequencies, necessitating a new search it. When synchronized and integrated with lethal fires, EA becomes a combat multiplier. EA can be used against computers, but it is not CNA. CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. Here are examples of each operation: Sending a code or instruction to a central processing unit that causes a computer to short out the power supply is CNA. Using an electromagnetic pulse to destroy a computer's electronics and causing the same result is EA. United States Army Intelligence and Security Command (INSCOM) is the Army's EA force provider (capabilities and units) and executor for Army and joint warfighters. Requests for EA should be forwarded through higher headquarters to United States Army Space Command (ARSPACE), where the EA coordination and planning process begins. Both are involved in Army EA planning and operations.

Staff Coordination

2-28. Staff responsibility for EW resides with the electronic warfare officer (EWO). Duties of the EWO as a special staff officer are listed in appendix F. The G-7 exercises coordinating staff responsibility over the EWO.

2-29. The EWO coordinates with the G-6 to deconflict EA targets with frequencies and the joint restricted frequency list. Together with the G-2

analysis and control element (ACE), the EWO identifies jamming, MD, and PSYOP targets. The EWO coordinates with the G-2 to deconflict/synchronize EW operations with intelligence collection operations, and for intelligence support to EW. The G-7 synchronizes CNA request with EW operations, deconflicting and synchronizing EW tasks with other IO tasks.

COMPUTER NETWORK OPERATIONS

2-30. ***Computer network operations*** **comprise computer network attack, computer network defense, and related computer network exploitation enabling operations.** CNO is not totally applicable at the tactical level. CNO is applicable at echelons above corps. CNA conducted in support of an Army service component command or its equivalent may affect lower echelons and support their objectives. CND is done at all army echelons across the spectrum of conflict. CNE is an intelligence function conducted at echelons above corps. (See definition at paragraph 2-43.)

COMPUTER NETWORK ATTACK

2-31. *Computer network attack* is operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (JP 3-13). CNA gives commanders with CNA release authority a nonkinetic strike option to enhance the effects of other lethal and nonlethal capabilities by destroying digital information. The G-7 is responsible for CNA planning and coordinates closely with the G-2, who begins the intelligence process to support CNA planning and operations, including battle damage assessment.

2-32. To maximize its effects, commanders integrate CNA with other IO elements. CNA can support, augment, and facilitate PSYOP and maneuver, deep strike, EW, fire support, and MD operations. Its capabilities include denying, deceiving, disrupting, and destroying adversary C2 nodes, weapon systems, communications systems, information, and networks. The G-7 looks for innovative ways to integrate its capabilities into the overall operation. IO planners coordinate and deconflict CNA and intelligence collection efforts. They also perform the following tasks:

- Determine desired CNA effects and their duration.
- Integrate CNA with other capabilities, lethal and nonlethal, to enhance its effects.
- Conduct a risk assessment to determine possible consequences of second- and third-order CNA effects.
- Deconflict potential CNA operations with CNE and other ongoing operations. Deconfliction includes an intelligence gain/loss assessment. The possible effects of a CNA operation on intelligence operations are a critical factor that commanders consider before executing it.

2-33. Most CNA are offensive IO. CNA targeted against resources the adversary requires to perform offensive IO is considered defensive IO.

2-34. Commanders consider its potential consequences before executing CNA. For example, a technologically advanced adversary that has refrained from conducting CNA may retaliate to friendly CNA in kind.

Contributions

2-35. CNA employs weapons that strike at the core attribute of an INFOSYS, connectivity, and its core function, C2 support. CNA has two objectives: deny or stop network service, and corrupt data. Of these two, data corruption has potentially the most disruptive effect on tactical C2, particularly if undetected.

Staff Coordination

2-36. Corps G-7s request CNA support from their joint task force or geographic combatant command headquarters through operations channels. The Secretary of Defense retains release authority for CNA execution. Upon approval, INSCOM initiates actions to begin Army CNA planning. (See appendix F.)

2-37. CNA are executed after careful policy and legal review. Commanders ensure any use of it is consistent with US international obligations and the law of war. Basic principles of the law of war—such as the requirements of military necessity, proportionality, and avoidance of undue suffering—apply to CNA.

COMPUTER NETWORK DEFENSE

2-38. *Computer network defense* consists of defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction (JP 3-51). It includes all measures to detect unauthorized network activity and adversary CNA and defend computers and networks against it. Such measures include access controls, malicious computer code and program detection, and intrusion-detection tools. CND is enabled by information assurance (IA). (See DODD O-8530.1.)

Contributions

2-39. To defend computer networks from unauthorized activity, each organization uses inherent capabilities to conduct CND. CND includes many responses to stop or minimize the effects of unauthorized activity. These include—

- Establishing protective measures within computer networks through network management (G-6) and information assurance (G-6 and G-7), procedures, tools, and trained personnel.
- Compiling and safeguarding information for tracking, apprehending and prosecuting perpetrators of unauthorized activity.
- Incorporating intrusion software into networks.
- Establishing firewalls.
- Increasing awareness training, including information from the G-2 on CND threats.

Staff Coordination

2-40. The G-6 has staff responsibility for CND at the tactical level. CND employs the capabilities of communications (G-6), law enforcement (Criminal Investigation Division (CID), and intelligence (G-2). System administrators ensure users follow appropriate procedures to prevent network intrusion.

2-41. The Army Computer Emergency Response Team (ACERT) deters, detects, coordinates, responds, and reports Army INFOSYS security incidents. Regional computer emergency response teams (RCERTs) deter, detect, coordinate, respond, and report Army INFOSYS security incidents. Both the ACERT and RCERTs unify CND efforts across networks. They assist G-6s in the war against hackers, intrusions, and viruses, and provide other technical assistance when needed. They co-locate with the United States Army Network Operations and Security Center (ANOSC; see appendix F), enabling the staffs to work closely together to protect networks and INFOSYS. Normally, the network operations (NETOPS) centers identify a potential network attack, either by direct observation or reports through the G-6 from impacted users, and pass it to the ACERT for a response. (See appendix F for command relationships.)

2-42. The complex nature of the Global Information Grid (GIG) requires close coordination of all CND activities between the operations, intelligence, communications, counterintelligence, law enforcement, and other government agencies.

COMPUTER NETWORK EXPLOITATION

2-43. ***Computer network exploitation*** **consists of enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.** (This definition is consistent with joint initiatives and is being staffed as a possible joint definition.)

Contribution

2-44. CNE contributes to intelligence collection at echelon above corps. (See appendix F for command relationships.)

SUPPORTING ELEMENTS

2-45. The supporting IO elements are physical destruction, IA, physical security, counterintelligence, counterdeception, and counterpropaganda. Physical destruction can be employed as an additional means to influence decisionmaker or groups, or to target INFOSYS in support of information superiority. Information assurance activities and network operations may be conducted independently or may be initiated in response to event-driven CND operational guidance. Physical security can support IO by preventing unauthorized physical access to personnel, equipment, installations, materiel, and documents. Counterintelligence investigations, operations, collection, analysis/production, and dynamic functional services can be employed in support of IO. Counterdeception contributes to situational understanding and defensive IO by protecting friendly C2 systems and decisionmakers from adversary deception. Counterpropaganda reduces the ability of adversary propaganda to influence friendly forces and others in the AO. It attacks adversary propaganda.

PHYSICAL DESTRUCTION

2-46. ***Physical destruction*** **is the application of combat power to destroy or degrade adversary forces, sources of information, command**

and control systems, and installations. It includes direct and indirect fires from ground, sea, and air forces. Also included are direct actions by special operations forces. The G-7 synchronizes execution of IO-related physical destruction with other IO elements and the fire support coordinator. Physical destruction is tied to critical events and decision points in the adversary decisionmaking processes or their underlying infrastructures. Artillery is a major, but not the only, contributor to this IO element. The targeting team assigns IO targets to the air and ground systems best able to attack them (see appendix E).

Contributions

2-47. When used as an IO element, physical destruction is normally offensive IO. Often destroying a target contributes to achieving both IO and conventional objectives. However, commanders use physical destruction as an IO element to disrupt, deny, degrade, or destroy the information, INFOSYS, the decisionmaking process, or the decisionmaker.

2-48. Traditional, attrition-based capabilities for physical destruction that can support IO include—

- Field artillery.
- Close air support.
- Army aviation.
- Special operations forces.
- Air defense artillery.
- EA (electromagnetic pulse, directed energy).
- Selected joint/national resources.
- Naval or strategic air assets.

Staff Coordination

2-49. The G-7 coordinates EW, PSYOP, OPSEC, and MD with physical destruction to achieve IO objectives (see JP 3-09; FM 6-20). The G-7 develops IO-related targets and enters them into the command targeting process (see appendix E).

INFORMATION ASSURANCE

2-50. *Information assurance* comprises information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (JP 3-13).

- *Availability* means timely, reliable access to data and services by authorized users. Available INFOSYS operate when needed.
- *Integrity* means protection from unauthorized change, including destruction. INFOSYS with integrity operate correctly, consistently, and accurately.
- *Authentication* means certainty of user or receiver identification and authorization to receive specific categories of information.
- *Confidentiality* means protection from unauthorized disclosure.

- *Nonrepudiation* means proof of message receipt and sender identification, so neither can deny having processed the data.

IA incorporates CND to provide a defense in depth that protects the GIG against exploitation, degradation, and denial of service by employing vigorous protection, detection, reaction, and restoration capabilities. This incorporation allows for effective defensive measures and/or timely restoration of debilitated networks and INFOSYS.

Contributions

2-51. IA attack contributes to defensive IO by protecting friendly information and INFOSYS against friendly intrusion as well as adversary attacks. IA uses a defense in depth that includes CND to counter adversary CNA.

2-52. IA defense in depth protects all networks, including their INFOSYS (such as computers and radios) and infrastructure implementation (such as gateways, routers, and switches). To contain damage and restore the networks, it provides information protection, intrusion/attack detection, and reaction.

2-53. Information protection is accomplished with a full range of security means. External and internal perimeter protection prevents unknown users or data from entering a network. External means include communications security; router filtering/access control lists, and security guards. Where necessary, physical isolation or barriers are placed between protected and unprotected networks. Internal perimeter protection consists of firewalls and router filters. These serve as barriers between echelons or functional communities.

2-54. Intrusion/attack detection is accomplished by monitoring the perimeter protection tools and devices to identify activities that violate security policies. Selected events or occurrences (such as numerous log-on attempts within a specific period) are monitored to detect unauthorized access and inadvertent, malicious, or nonmalicious modification or destruction of data.

2-55. Network managers react to counter the effects of an incident on the network. Reaction to a network or INFOSYS intrusion incorporates the capability to restore essential information services, as well as initiate attack response processes. Disaster recovery capability requires stopping the breach and restoring the network. A detailed continuity of operations plan facilitates accomplishing these tasks.

2-56. The Army INFOSYS Security Program addresses security measures that protect information and INFOSYS against all forms of threats (see AR380-19). System development requires INFOSYS security planning during acquisition, training, development, operations, and maintenance. When the program is properly functioning, an in-depth system provides protection and defense of information and INFOSYS (see *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations* for details).

Staff Coordination

2-57. The G-6 is responsible for IA. IA is one of the components of NETOPS as is network management and information dissemination management. The IA manager, IA network manager, IA security officer, systems administrator,

and other G-6 staff members help the assistant chief of staff G-6 execute the IA/NETOPS mission. The G-6 coordinates with the G-5 on the availability of commercial INFOSYS and services for military use. The G-5 identifies and assists the G-6 with coordination for military use of local communications systems. The EWO coordinates with the G-6 to deconflict frequencies for EA targets to ensure friendly IA is not affected. The G-2 provides information and intelligence regarding threats to Army information and INFOSYS. The G-7 deconflicts IA with the other IO elements.

2-58. The G-6 disseminates the information operations condition (INFOCON) to units and the staff. The INFOCON provides a coordinated structured approach to defense against, and reaction to, attacks on computers, networks, and INFOSYS. The INFOCON statuses and their associated actions are—

- Normal (no significant activity).
- Alpha (increased risk of attack).
- Bravo (specific risk of attack).
- Charlie (limited attack).
- Delta (general attack).

2-59. **Normal (no significant activity)**. Under INFOCON Normal, organizations take the following actions:

- Ensure all mission-critical information and INFOSYS (including applications and databases) and their operational importance are identified.
- Ensure all points of access and their operational necessity are identified.
- On a continuing basis, conduct normal security practices.
- Conduct periodic internal security reviews and external vulnerability assessments.

2-60. **Alpha (increased risk of attack)**. INFOCON Alpha is imposed when—

- Indications and warning indicate a general threat.
- Regional events are occurring which affect U.S. interests and involve potential adversaries with suspected or known CNA capabilities.

2-61. INFOCON Alpha actions include—

- Increasing security for INFOSYS supporting planned or ongoing operations, contingencies or exercises for INFOSYS.
- Executing appropriate security practices; for example, increasing the frequency of audit, review, and critical file back-up procedures.
- Accomplishing all actions required at INFOCON Normal.

2-62. **Bravo (specific risk of attack)**. INFOCON Bravo is imposed when—

- Indications and warning indicate that a specific system, location, unit, or operation is being targeted.
- A significant level of network probes, scans, or activities indicating a pattern of concentrated reconnaissance are detected.
- Network penetrations or denial-of-service attacks are attempted but have no impact to DOD operations.

2-63. INFOCON Bravo actions include—

- Executing appropriate defensive tactics.

- Executing appropriate security practices; for example, conducting immediate internal security reviews of all critical systems.
- Accomplishing all actions required at INFOCON Alpha.

2-64. **Charlie (limited attack)**. INFOCON Charlie is imposed when—

- Intelligence attack assessment indicates a limited attack is underway.
- An INFOSYS attack with limited impact on DOD operations is detected; for example, little or no data or systems are compromised.

2-65. INFOCON Charlie actions include—

- Execute the maximum level of auditing, review, and critical file back-up procedures.
- Consider imposing MINIMIZE on appropriate computer networks and telecommunications systems. (MINIMIZE limits traffic to mission-essential communications only.)
- Reconfigure INFOSYS to minimize access points and increase security.
- Reroute mission-critical communications through unaffected systems.
- Execute defensive tactics; for example, ensure increased reporting requirements are met.
- Accomplish all actions required under INFOCON Bravo.

2-66. **Delta (general attack)**. INFOCON Delta is imposed when—

- A successful INFOSYS attack that impacts DOD options is detected.
- Widespread incidents that undermine the ability of targeted INFOSYS to function effectively occur.
- The effects of attacks or incidents produce a significant risk of mission failure.

2-67. INFOCON Delta actions include—

- Execute the applicable portions of continuity of operations plans. For example designate alternative INFOSYS and disseminate new communication internal and external procedures. Isolate compromised systems from the rest of network.
- Accomplish all actions required under INFOCON Charlie.

2-68. United States Strategic Command (STRATCOM) establishes the INFOCON. When the INFOCON changes, STRATCOM notifies the ACERT (see appendix F). The ACERT passes the new INFOCON to corps and division G-6s.

PHYSICAL SECURITY

2-69. *Physical security* is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (JP 3-13). Effective physical security ensures the availability of INFOSYS used to conduct operations**.** It is based on—

- Identifying mission-essential INFOSYS.
- Determining applicable risks and threat levels.
- Establishing relative security standards and using available resources to achieve that level of physical security.

- Determining applicable protection levels.
- Coordinating with higher and adjacent units and host-nation agencies.
- Developing contingency plans for natural disasters, terrorist actions, or weapons of mass destruction attacks.

See AR 190-13 and FM 3-19.30 for physical security requirements and TTP.

Contributions

2-70. Commanders conduct physical security operations to safeguard resources, including information and INFOSYS. Properly integrated, physical security complements the other IO elements.

2-71. Physical security resources include the following:

- **Physical security programs**. Commanders establish physical security programs appropriate to their command's mission.
- **Physical security specialists**. Physical security specialists from the provost marshal staff can identify vulnerable areas and recommend appropriate countermeasures. Additionally, they can provide assessments of unit physical security measures.

2-72. The G-7 synchronizes physical security measures with other IO element operations. First-line leaders ensure soldiers know regulatory requirements, understand how physical security measures protect information and INFOSYS, and learn to recognize potential problem areas in physical and information security.

Staff Coordination

2-73. The provost marshal holds staff responsibility for physical security. At echelons where no provost marshal is authorized, the G-2 assumes this responsibility He conducts physical security operations to protect critical assets, nodes, and sensitive materials. He coordinates with other staff offices for physical security matters. The G-2 assesses physical security vulnerabilities. The provost marshal informs the G-7 of suspected physical security violations involving the elements of IO. He advises the G-6 of those involving IM.

COUNTERINTELLIGENCE

2-74. *Counterintelligence* is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 3-13).

Contributions

2-75. Counterintelligence (CI) operations support preserving essential security and protect the force, directly and indirectly (see JP 2-01.2; FM 34-60). They are tailored to the sensitivity of the unit and its vulnerability to adversary intelligence surveillance and attack.

2-76. The CI mission is to detect, identify, assess, counter, neutralize, or exploit hostile intelligence collection. CI personnel are part of a vulnerability

assessment team (along with the provost marshal, engineers, medics, and other personnel, as required). Normal CI activities also contribute to both offensive and defensive IO. CI personnel do this through—

- Supporting information security, particularly through the enforcement of regulation and conduct of investigations pertaining to failures in proper handling of classified and compartment information.
- Providing input to the analysis conducted to identify adversary human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT) collection.
- Providing to the command a picture of its susceptibility to foreign intelligence collection.
- As appropriate, provides support to MD operations.

2-77. It is necessary to distinguish between the counterintelligence discipline, and the counterintelligence military occupational specialty (MOS). Principles of the counterintelligence discipline apply across the spectrum of intelligence collection efforts, MD operations, security and other functions of both maneuver and intelligence units. For example, OPSEC is designed to counter the enemy's ability to collect on friendly force activities; it is an application of the principle of counterintelligence discipline. Planning, performing, and enforcing OPSEC does not require an accredited CI agent. On the other hand, CI agents who possess the MOSs 97B, 351B, or 35E are those actual agents on the ground who conduct investigations, operations, and who participate with other staff elements in the conduct of vulnerability assessments.

Staff Coordination

2-78. The G-2 monitors CI operations conducted within the AO. The G-2 keeps the commander and staff informed as appropriate concerning CI operations and their potential effect on other friendly functions, as well as adversary capabilities and intent.

COUNTERDECEPTION

2-79. *Counterdeception* consists of efforts to negate, neutralize, diminish the effects of, or gain the advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations (JP 3-13).

Contributions

2-80. Counterdeception contributes to situational understanding and defensive IO by protecting friendly C2 systems and decisionmakers from adversary deception. Its goal is to make friendly decisionmakers aware of adversary deception activities so they can formulate informed and coordinated responses.

2-81. Counterdeception strives to identify and exploit adversary attempts to mislead friendly forces. Activities that contribute to understanding adversary posture and intent serve to identify adversary deception attempts.

2-82. Countering deception is difficult. Knowing deception methods an adversary has used successfully is important. Properly balancing tactical and

operational indicators with strategic assumptions is also important. The chance of surprise might be reduced if estimates weigh tactical indicators more heavily than strategic assumptions. Dismissing tactical indicators because they conflict with preconceptions may allow a hostile deception operation that plays on those preconceptions to succeed.

2-83. Offensive counterdeception includes actions taken to force adversaries to reveal their actual and deception intentions and objectives. It focuses on forcing an adversary to expend resources and continue deception operations that have been detected by reinforcing the perception that friendly forces are unaware of them. Counterdeception includes actions taken to thwart adversary attempts to capitalize on deception tactics, thus affecting adversary decisionmaking processes.

Staff Coordination

2-84. The G-2 and G-7 determine indicators of adversary deception activities. The G-2 incorporates information requirements that identify these indicators into the collection plan. The G-2 is responsible for detecting adversary deception operations. The G-7 coordinates the counterdeception response. Coordinating and special staff officers act within their fields of interest to negate, neutralize, and diminish adversary deception activities. The G-7 synchronizes these actions.

COUNTERPROPAGANDA

2-85. *Counterpropaganda* consists of programs of products and actions designed to nullify propaganda or mitigate its effects (FM 3-05.30). It is directed toward the target of adversary propaganda. Counterpropaganda degrades the harmful influence of adversary PSYOP on friendly forces and other audiences (see JP 3-53; FM 3-05.30; FM 33-1-1).

2-86. The increasingly complex nature of military operations confronts Army forces with new challenges. Nowhere is this challenge greater than in counterpropaganda. Counterpropaganda includes countering adversary misinformation, disinformation, and opposing information. PSYOP forces attached to divisions and corps are responsible for counterpropaganda. Counterpropaganda applies across the range of operations and spectrum of conflict. It counters messages, images, rumors, and other information that aim to impede or prevent friendly mission accomplishment. Examples of adversary propaganda include the World War II radio broadcasts of Lord Haw Haw (William Joyce) to the British Isles during the Battle of Britain, and the radio broadcasts by Tokyo Rose in the Pacific Theater.

2-87. *Propaganda* is any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly (JP 3-53). It is normally directed at the United States, multinational partners, and key audiences in the AO. Propaganda campaigns are deliberately designed to attack the will of nations to resist and soldiers to fight. Propagandists seek to mix truth and lies in a way that listeners cannot detect.

2-88. ***Misinformation*** **is incorrect information from any source that is released for unknown reasons, or to solicit a response or interest**

from a nonpolitical or nonmilitary target. The target of this information can be anyone. Misinformation is often best countered by either ignoring it altogether or disseminating the truth. However, even providing the facts can consume resources and time, and may not be worth the effort. In some situations, the credibility of the military is pitted against a credible news agency, and there may be no clear winner. Therefore, it is often best to be open and objective when faced with possible misinformation. A cooperative relationship between the military PA staff and the media may help counter the effects of misinformation.

2-89. ***Disinformation*** **is information disseminated primarily by intelligence organizations or other covert agencies designed to distort information, or deceive or influence United States decisionmakers, United States forces, coalition allies, key actors, or individuals by indirect or unconventional means**. It is a form of propaganda directed toward decisionmakers to confuse them into making incorrect decisions. At the tactical level disinformation can lead commanders to expend resources to guard against nonexistent threats. Disinformation can cause rifts in coalitions by playing off historical ethnic, racial, and cultural biases of coalition partners. Adversaries can direct disinformation indirectly, such as through third-party communications broadcasts. They may also use unconventional means, such as notices on common-use items like matchboxes or novelty gifts.

2-90. ***Opposing information*** **is intentional or unintentional truth-based information from any source that represents an opposing view**. It is usually directed against the US military, allies or multinational partners, and key audiences within the AO. However, it may be directed at adversaries, potential adversaries, or nonaligned parties. Opposing information requires US decisionmakers to understand the effects US forces produce in an AO, and act to minimize negative images of US policy and operations and amplify positive images.

2-91. Countering propaganda in a foreign AO is usually the responsibility of PSYOP units. Other government agencies counter propaganda outside the AO. Often, PSYOP forces depend on the information networks of allies or multinational partners to counter propaganda within their borders. However, PSYOP forces may provide assistance when requested.

2-92. The ideal counterpropaganda plan incorporates efforts of a loose network of organizations and agencies. It often provides common themes and objectives. All IO elements support counterpropaganda plans, but PSYOP forces usually conduct counterpropaganda operations.

2-93. Adversaries, potential adversaries, and the other groups use propaganda, misinformation, and disinformation to influence public opinion, the international media, and friendly decisionmakers. Commanders use counterpropaganda to provide targeted audiences with an alternative information source. Counterpropaganda preempts, prevents, and disrupts adversary efforts to disseminate propaganda, misinformation, and disinformation. At the tactical and operational levels, the focal point for counterpropaganda may vary, based on mission, enemy, terrain, troops and time available and civil

considerations (METT-TC). However, the G-7 retains primary staff responsibility and oversight.

2-94. Good policies and actions taken by a military force, the government, or multinational partners may produce adverse effects. When American troops deploy overseas, their presence can create problems. For example, one foreign humanitarian assistance operation created economic hardships for the civil population in the AO, even though the mission was to build schools and hospitals. Local leaders complained that the force bought all the construction materials in the area, which drove up prices. Local businessmen complained that Americans were signing contracts and working with minority and small businesses rather than with them. In situations like this, opposing attitudes and beliefs can create an image of the force that nullifies its success, if not detected and addressed quickly. Normally, PSYOP units create the image of the force with support from the PA and CMO.

2-95. Countering information disseminated within the United States is not the armed forces responsibility. Countering information directed towards strategic audiences (essential leaders, officials, and agencies) remains the responsibility of the State Department and the International Broadcasting Board. Commanders coordinate counterpropaganda activities through PSYOP channels and the geographic combatant command IO cell. However, strategic counterpropaganda is normally conducted by the State Department and coordinated by the Joint Chiefs of Staff through the International Public Information Committee.

Contributions

2-96. Counterpropaganda reduces the ability of adversary propaganda to influence friendly forces and others in the AO. It attacks adversary propaganda.

2-97. Counterpropaganda includes preventive actions, counteractions, and rumor control. Preventive actions take the form of propaganda awareness programs. These programs inform US and multinational forces, and friendly populations about the nature of hostile propaganda. Counteractions are measures that PSYOP units take to reduce or neutralize the effects of hostile propaganda. Rumors are a means of propaganda by based on widely disseminated talk or opinion. They have no discernable source and no known authority. Rumor control seeks to counter rumors that are unfavorable to U.S interests.

2-98. Failure to counter adversary propaganda can produce many effects. These range from simple confusion to disrupting ongoing operations. Common effects of hostile propaganda, misinformation, and disinformation, include—

- Prompting neutral parties to resist or not support military operations.
- Increasing adversary will to resist by fanning hatreds, biases, and predispositions.
- Leading multinational partners to question their roles in a coalition.
- Inciting riots.
- Causing refugees to block lines of communication.

- Fostering distrust for US or US-led forces.
- Causing host nations or other nonbelligerent parties to not cooperate with friendly forces.
- Causing essential communicators to resist or deny cooperation.
- Causing diversion of military assets to address problems that, while seemingly insignificant, require significant resources.
- Leading friendly governments to questions their own policies and support for military operations.

Seizing the Initiative: Counterpropaganda in a Peace Operation

Counterpropaganda operations can involve more than leaflets and broadcasts. The On 11 November 1998, US soldiers serving with Task Force Eagle of the NATO Stabilization Force in Bosnia (SFOR) held a meeting in the town of Dizdarusa to inform the citizenry about displaced person and refugee resettlement in their area. Five Bosnian Serbs disrupted the meeting and threatened the Bosnian Muslims in attendance. The US soldiers immediately took photographs of three of the intruders to document their illegal actives, but two departed before the soldiers could photograph them. Upon determining the identities of the remaining perpetrators, a patrol from Camp McGovern went to their homes and delivered a message through an interpreter that SFOR would not tolerate violence. The soldiers then photographed them. The *Stars and Stripes* interviewed the Task Force Eagle commander and published a balanced and accurate story. When the Bosnian Serb newspaper, *Gras Srpski*, published an account of the incident that the SFOR soldiers as abusing their power, Task Force Eagle held a press conference with the Breko area media to refute the story. These aggressive actions allowed Task Force Eagle to maintain the initiative in a situation where accomplishing the mission required disseminating accurate information and refuting false allegations.

Staff Coordination

2-99. Though PSYOP forces take the lead in counterpropaganda operations, PA personnel play an important role. For example, if adversary elements accuse friendly forces of committing atrocities, PSYOP forces may disseminate products refuting the charges, while PA personnel present accurate information directly to the media. Although PA's primary target audience is the American public and internal audiences, the secondary target audience is the belligerent government and its civil population. Properly synchronized PSYOP and PA operations complement each other.

2-100. The G-7 coordinates responses to adversary propaganda. The G-7 also coordinates support with higher headquarters PSYOP elements. The geographic combatant commander approves counterpropaganda tasks.

RELATED ACTIVITIES

2-101. Related activities include, but are not limited to, PA and CMO. PA and CMO can create conditions that contribute to information superiority.

They contribute to support of Army operations by US and international audiences, and maintain relations with the civilian populace in the AO.

2-102. Effective PA truthfully inform the public. They do not focus on directing or manipulating public actions or opinion. PA help shape the information environment. It can serve to counter adversary propaganda, and disinformation.

2-103. CMO can support IO objectives by influencing, developing, or controlling the indigenous infrastructure in foreign AOs. It can be an alternative means to communicate with the host nation and foreign public.

PUBLIC AFFAIRS

2-104. *Public affairs* are those public information, command information, and community relations' activities directed toward both the external and internal publics with interest in the Department of Defense (JP 3-61). (Army doctrine uses the term *internal information* in place of *command information*.) PA information is credible. It makes available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy. Effective PA enhances confidence in the force and its operations (see JP 3-61; FM 46-1; FM 3-61.1).

Contributions

2-105. PA fulfills the Army's obligation to keep the American people and the Army informed. It helps establish conditions that lead to confidence in the Army and its readiness to conduct operations during peace, crisis, and war. PA keeps all members of the force informed, and counters the effects of adversary propaganda and misinformation.

2-106. PA supports IO by producing accurate, timely, and balanced information for the public, explaining—after the fact—the objectives of an operation. Public affairs supports both offensive IO and defensive IO. PA support to offensive IO takes the form of active measures, such as press conferences, press releases, articles, and specific talking points. Defensive IO includes products such as media guidance, researched answers to probable media questions, and crisis reporting plans for high profile incidents. PA personnel also review IO products from a media perspective to suggest improvements.

2-107. PA principles that support IO are as follows:

- **Truth is paramount**. Successful and effective public relations depend on credibility. The quickest way to destroy PA credibility is to misrepresent the truth. Close coordination within the IO cell is required to ensure that the media and the US and multinational publics are not deceived or lied to, and that such a perception is not created.
- **If news (information) is out, it is out**. The information environment makes information readily available and enables fast, easy dissemination. Once information is released, it must be assumed that it is available to all interested audiences. DOD policy prohibits withholding or classifying information to prevent criticism or embarrassment.

- **Deploy PA assets early**. The media may be in the AO before Army forces arrive and may be well established there. Media interest is intense during initial force deployment and the onset of operations. PA assets are needed at the earliest stages to ensure effective IO.
- **Practice security at the source**. Any form of field censorship is impractical technically and unacceptable politically. All soldiers and Army civilians are trained and provided with PA guidance for potential interaction with civilian media. Family members are provided with guidance in dealing with the civilian media. Even so, the standard is not to share any information that by policy or law is deemed inappropriate for release.
- **Speak with one voice**. PA assets are integrated at all echelons. Commanders train soldiers to talk only about what they know within their own responsibilities and not to speculate about other areas.

Maintaining the Initiative at Home Station

A commander's battlespace includes the home station. Commanders act to shape the information environment there as well as in the AO. During Operation Joint Forge, the commanding general of the first CONUS-based division to deploy to Bosnia used weekly video teleconferences with the rear detachment and unit family readiness group as part of an overall internal information (formerly command information) program. The CG used this medium to provide internal information to families, and to quell rumors, misinformation, and potential disinformation at home station. The G-1 and PA officer shared responsibility for managing video teleconferences. The G-6 assisted them. During these video teleconferences, the commanding general personally asked, "What are the rumors back there?" He then provided answers to the assembled family readiness group representatives, spouses, and local community representatives. Video teleconferences such as these incorporate aspects of PA and counterpropaganda. They are one means that commanders use to maintain the initiative in the information environment.

2-108. PA personnel help commanders shape the information environment by preparing command themes and messages, and conducting media analysis. Command themes and messages support IO by countering enemy propaganda and disinformation, highlighting the force effectiveness, and quickly responding to mistakes or failures. Disseminating them throughout the force allows contacts with target audiences by any element of the force to be an opportunities to reinforce that image. Conveying consistent messages to local populations is especially important during peace operations and some support operations. These messages should be updated to keep them relevant to the situation. PA personnel create a media analysis plan for later assessment of outputs. They do this in the context of agreed-upon themes and command directives.

2-109. PA personnel create a media analysis plan and conduct media analysis to assess the success, strengths, and weaknesses of their PA actions and the impact on the IO concept of support. This information provides a sense of the issues the local population's attention is focused on. PA personnel analyze information and determine releasable material of items that have potential media interest while working closely with intelligence personnel.

Staff Coordination

2-110. PA, PSYOP, and CMO communicate information to influence audience understanding and perceptions of operations. They are coordinated to eliminate unnecessary duplication of effort, ensure unity of purpose, and ensure credibility is not undermined.

CIVIL MILITARY OPERATIONS

2-111. *Civil military operations* are activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational United States objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. 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 (JP 3-57).

2-112. CMO encompass all aspects of the civil dimension that commanders must address to accomplish their mission. These aspects include, but are not limited to, the local civilian populace and government, nongovernmental organizations, and international organizations that may affect or influence military operations. CMO supports restoration of the indigenous communications infrastructure and engages the cultural, social, political, and economic sectors in the AO (see JP 3-57; FM 41-10).

Contributions

2-113. CMO have two forms: support to military operations and support to civil authorities.

2-114. **Support to Military Operations**. Support to military operations seeks to minimize civilian interference with military operations, maximize support for operations, and meet the commander's legal responsibilities and moral obligations to civilian populations within the AO. Operationally, CMO supports national policy and implements US national objectives by coordinating with, influencing, developing, or accessing indigenous infrastructures in the AO. Tactically, CMO secure local acceptance of and support for US forces. It is important to IO because CMO involve interfacing with essential organizations and individuals in the AO and with nongovernmental organizations, such as the International Committee of the Red Cross.

2-115. **Support to Civil Authorities**. Support to civil authorities includes assistance with relief, dislocated civilian support (dislocated persons, evacuees, expellees, or refugees), and security or technical assistance. These activities may include such actions as—

- Coordinating the removal of civilians from the combat zone.
- Interfacing between US/multinational forces and host nation and other governmental/nongovernmental organizations.
- Exercising military control over an area, hostile government, or population.

2-116. **Limitations on Using Civil Affairs Forces**. *Civil affairs* forces are designated active and reserve component forces and units organized, trained, and equipped specifically to conduct civil affairs activities and to support civil-military operations (JP 3-57). The need of CA forces to maintain credibility with the civil populace limits the extent to which they can support IO. The daily encounters between CA soldiers and the people and institutions of the AO are prime sources of information. CA soldiers collect this information and conduct assessments in order to target their relief efforts or stabilize the civil environment. CMO support IO and facilitates mission accomplishment by enhancing the relationship between the overall force and the civilian populace. However, CA units avoid any perception that their activities are related to IO.

Civil Military Operations is a Peacekeeping Environment

CMO during peace operations include civil-military information programs that inform the local populace about ongoing military operations and secure their acquiescence and noninterference. An example of such an operation was the mine-awareness puppet show presented to Bosnian children in Multinational Division-North AO. Task Force Eagle CA soldiers produced a puppet show that was shown to children throughout AO. The Coalition Press Information Center provided publicity. The CA unit supporting Task Force Eagle used volunteer soldiers to present the puppet show with the assistance interpreters. The puppet shows were given to local school children in groups as large as 100. The puppets represented people of different colors and ethnic backgrounds. Themes focused on diverse people living together in peace and harmony. The puppet show was very popular with the children, who seemed to understand and accept the moral lessons it presented. Additionally, the puppet show provided opportunities for civil affairs personnel to meet and talk to mayors and other local leaders, who otherwise would have been inaccessible.

Staff Coordination

2-117. Public affairs, PSYOP, and CMO are coordinated to eliminate unnecessary duplication of effort, ensure unity of purpose, and ensure credibility is not undermined.

- The G-7 coordinates activities supporting IO objectives and CMO tasks with the G-5.
- The G-5—
  - Provides recommended CMO-related information requirements and EEFI to the G-7.
  - Coordinates with the G-2 on aspects of the enemy situation that may affect CMO.
  - Coordinates for tactical forces to perform CMO tasks with the G-3.
  - Identifies and assists the G-6 with coordination for military use of local communications systems.
  - Coordinates with the G-7 on trends in public opinion.
  - Coordinates with the G-7 and PAO to ensure disseminated information is truthful and supports IO objectives.
  - Coordinates with the PAO on supervising public information media.

	OPSEC	Military Deception	PSYOP	Physical Destruction	EW	Physical Security
OPSEC supports by		• Concealing competing observables • Degrading general situation information to enhance effect of observables • Limiting information and indicators that could compromise MD operations	• Concealing contradicting indicators while conveying selected information and indicators	• Concealing friendly delivery systems from enemy offensive IO until it is too late for the adversary to react • Denying information to enemy on the success of enemy offensive IO	• Concealing EW units and systems to deny information on extent of EA/ES capabilities	• Concealing EEFI • Reducing the activities requiring physical security • Hiding tools of physical security thus preventing adversary from gaining access
Military deception supports by	• Influencing adversary not to collect against protected units/activities • Cause adversary to underestimate friendly OPSEC capabilities		• Providing information compatible with PSYOP theme	• Influencing adversary to underestimate friendly physical destruction capabilities • Influencing adversary to defend C2 elements/systems that friendly forces do not plan to destroy	• Influencing adversary to underestimate friendly EA/ES capabilities	• Masking troop activities requiring safeguards
PSYOP supports by	• Disseminating ROE • Countering propaganda and misinformation • Minimizing resistance and interference by local population	• Creating perceptions and attitudes that MD can exploit • Integrating PSYOP actions with MD • Reinforcing the deception story with information from other sources		• Causing populace to leave targeted areas to reduce collateral damage	• Broadcasting PSYOP products on adversary frequencies • Developing messages for broadcast on other service EW assets	• Targeting adversary audiences to reduce the need for physical security
Physical destruction supports by	• Preventing or degrading adversary reconnaissance and surveillance	• Conducting physical attacks as deception events • Degrading adversary capabilities to see, report, and process observables	• Degrading adversary ability to see, report, and process information • Degrading adversary ability to jam PSYOP broadcasts		• Destroying adversary C2 targets • Destroying electronic systems adversary use	• Reducing physical security needs by attacking adversary systems able to penetrate INFOSYS

Figure 2-1. Mutual Support within IO Elements

	OPSEC	Military Deception	PSYOP	Physical Destruction	EW	Physical Security
EW supports by	• Degrading adversary electromagnetic ISR operations against protected units and activities • Creating barrier of white noise to mask unit maneuvers	• Using EA/ES as deception measures • Degrading adversary capabilities to see, report, and process competing observable. • Causing enemy to misinterpret information received by his electronic means	• Degrading adversary's ability to see, report, and process information • Isolating target audience from information	• Providing target acquisition through ES • Destroying or upsetting susceptible assets with EA		• Using EP to safeguard communications used in protecting facilities
IA supports by	• Ensuring INFOSYS confidentiality	• Providing INFOSYS assets for conducting MD operations	• Ensuring availability of INFOSYS for PSYOP	• Ensuring INFOSYS are available for physical destruction tasks	• Ensuring EW assets are available	• Providing for INFOSYS authentication
CNA supports by	• Attacking enemy computers before they can detect our EEFI	• Providing the deception story through computers	• Another means of providing the PSYOP theme	• Nonlethal attack of selected targets, which allows lethal attacks on other targets	• Used with EA	• Conducting risk assessment to determine consequence of 2d and 3d order CNA effects
CND supports by	• Detecting enemy attempts to acquire information	• Protecting the MD plan resident inside computers	• Preventing the compromise of PSYOP message before release	• Protecting fire support C2 systems	• Used in conjunction with EP	• Erect firewalls to prevent intrusion into networks
Physical security supports by	Protecting OPLANs/ OPORDs	• Restricting access by level of security and number of personnel	• Ensuring products do not contain classified information	• Safeguarding availability of INFOSYS to use in physical destruction	• Safeguarding equipment used in EW	
Counter-deception supports by	• Providing a cover story for unit operations	• Enhancing friendly MD operations by deceiving the enemy on the impact of his deception	• Neutralizing or diminishing foreign deception operations	• Identifying adversary deception targets so physical destruction can be used against them	• Identifying adversary deception targets so EW can be used against them	• Determine enemy deception before physical security is compromised
Counter-propaganda supports by	• Emphasizing need for OPSEC	• Providing deception targets	• Providing PSYOP targets	• Providing physical destruction targets	• Providing EA targets and emphasizing EP	• Reduce the number of facilities to be secured by exposing enemy lies
Counter-intelligence supports by	• Countering foreign HUMINT operations	• Countering foreign HUMINT operations • Identifying threat ISR capabilities	• Conducting Countersignal operations to allow broadcast of PSYOP messages	• None	• Providing electronic countermeasures	• Countering foreign HUMINT operations

Figure 2-1. Mutual Support within IO Elements (continued)

	IA	Counter-Deception	Counter-Propaganda	CI	CNA	CND
OPSEC supports by	• Concealing physical and electronic INFOSYS locations	• Concealing the true commander's intent	• Decreasing number of activities subject to enemy propaganda	• Ensuring EEFI are concealed from enemy collection assets	• Concealing CNA capabilities	• Denying enemy knowledge about CND capabilities
Military deception supports by	• Overloading adversary intelligence and analysis capabilities • Protecting/defending friendly INFOSYS	• Causing adversary to employ forces in ways that reinforce counter-deception activities • Deceiving adversary on results of his deception	• Inducing the adversary to use inappropriate propaganda, thus exposing him to counterpropaganda	• Giving the adversary a cover story so his intelligence system collects irrelevant information	• Providing MD targets and deception stories to enhance CNA	• Causing enemy to believe our CND is greater than it acutally is • Cause enemy to believe all CND tools are in place
PSYOP supports by	• Enhancing the ability of IA in the minds of the enemy	• Assessing psychological impact of counterdeception activities on adversary • Detecting adversary deceptions	• Countering hostile propaganda	• Providing messages in enemy decisionmaker's mind that can be revealed by CI to determine enemy true intentions	• Convincing enemy not to do something by describing effects of a CNA if they take undesirable actions	• Providing information about non-military threat to computers in the AO
Physical destruction supports by	• Attacking adversary systems capable of influencing friendly INFOSYS availability and integrity	• Negating or neutralizing adversary deception capabilities	• Destroying communication facilities capable of transmitting propaganda	• Destroying appropriately nominated adversary collection assets	• Supplementing CNA by destroying or degradeing hard targets	• Destroying or degading enemy CNA facilities before they attack friendly computers
EW supports by	• Using EP to protect equipment	• Conducting EA against adversary deception capabilities	• Conducting EA to reduce adversary electromagnetic spectrum use	• None	• Supplementing CNA with EA	• Using EP to protect personnel, facilites and equipment
IA supports by		• Providing INFOSYS integrity ensuring INFOSYS are not deceived	• Providing for nonrepudiation of information	• Ensuring INFOSYS are available to conduct CI	• Ensuring links with higher HQ to pass CNA requests	• Taking actions to ensure availabilitiy, integrity, authentication, confidentiality, and nonrepudiation of computers
CNA	• Attacking enemy computers before enemy attacks friendly computers	• Exploit enemy attempts to mislead friendly forces	• Attacking enemy propaganda disseminators	• Exploiting enemy intelligence collection		• Attacking enemy ability to attack friendly computers
CND	• Supporting IA of information passed via computer networks	• Filtering enemy deception data prior to being given to decision-makers	• Ensuring truthful friendly computer information thus negating enemy PSYOP	• Detecting, identifying, and assessing enemy collection efforts against computers	• Protecting CNA weapons from enemy detection	

Figure 2-1. Mutual Support within IO Elements (continued)

	IA	Counter-deception	Counter-propaganda	CI	CNA	CND
Physical security supports by	• Safeguarding INFOSYS by implementing security procedures	• Safeguarding installations and materiel from enemy deception	• Safeguarding personnel from espionage	• Safeguarding personnel, and preventing unauthorized access to equipment, installations, materiel, and documents	• Safeguarding INFOSYS from sabotage, espionage, damage, or theft	• Determining applicable risk and threat levels
Counterdeception supports by	• Preventing enemy from interfering with authentication and confidentiality of information		• Confirming truthful information from two means	• Confirming enemy intentions from two means	• Negating, neutralizing or diminishing an enemy deception operation against CNA	• Negating, neutralizing or diminishing an enemy deception operation against CND
Counterpropaganda supports by	• Providing truth on enemy intentions to systems administrators responsible for IA	• Countering rumors		• Educating populace about rumors	• Countering disinformation about enemy CND	• Countering enemy propaganda
CI supports by	• At certain echelons, helping ensure information integrity	• Identifying and neutralizing adversary HUMINT collection capability	• Identifying sources of deception activities		• Confirming results of CNA	• Detecting, identifying, assessing, countering, neutralizing enemy intelligence collection

Figure 2-1. Mutual Support within IO Elements (continued)

	OPSEC	Military Deception	PSYOP	Physical Destruction	EW	Physical Security
OPSEC can conflict by		• Limiting information that can be revealed to enhance deception story credibility	• Limiting information that can be revealed to develop PSYOP themes	• Limiting information that can be revealed to enemy to develop targets	• EP and OPSEC may have different goals	• Should be no conflict
Military deception can conflict by	• Revealing information OPSEC normally seeks to conceal		• Limiting PSYOP theme selection • Limiting information that can be revealed to develop PSYOP themes	• Limiting targeting to allow survival and conduct of critical adversary C2 functions	• Limiting EA targeting of adversary INFOSYS to allow survival and conduct of critical adversary C2 functions	• Negating the deception story by physical security preventing our transmitting a realistic deception story
PSYOP can conflict by	• Revealing information OPSEC normally seeks to conceal	• Limiting deception story selection • If deception story contains untruths		• Limiting targeting of adversary C2 infrastructure to allow conveying PSYOP themes	• Limiting EA against adversary communications frequencies to allow PSYOP themes to be conveyed	• Should be no conflict
Physical destruction can conflict by	• Causing firing systems to reveal their locations	• Limiting selection of deception means by denying or degrading elements of adversary C2 infrastructure necessary to process deception story	• Limiting means available to convey PSYOP themes by denying or degrading adversary C2 systems		• Limiting opportunities for communications intrusion by denying or degrading elements of adversary INFOSYS	• If need-to-know considerations limit access to targeting data
EW can conflict by	• Revealing EW assets prematurely	• Limiting selection of deception measures by denying or degrading use of adversary C2 systems	• Reducing frequencies available to convey PSYOP themes	• Limiting targeting of adversary C2 systems		• Revealing what physical security is trying to protect (EA) • EP should not conflict
IA can conflict by	• Should be no conflict	• Limiting means of transmitting the deception story	• Should be no conflict	• Should be no conflict	• EP and IA must be deconflicted	• Should be no conflict
CND can conflict by	• Should be no conflict	• Reinforcing the deception story	• Should be no conflict	• Should be no conflict	• Should be no conflict	• Should be no conflict

Figure 2-2. Potential Conflicts within the Elements of IO

	OPSEC	Military Deception	PSYOP	Physical Destruction	EW	Physical Security
CNA can conflict by	• Attack selected on enemy targets may provide information on friendly activities	• May result in attacking wrong target if coordination not made with MD	• Preventing the enemy from receiving the PSYOP message	• Attack same target with nonlethal and lethal weapons wastes both time and ammo	• Need to deconflict which systems attack which targets	• Reveiling CNA source that should be protected
Counterdeception can conflict by	• Should be no conflict	• Not providing to deception planners the correct enemy deception	• May cause wrong message being used	• Inadvertently hitting civilians with friendly fire can cause strategic repercussions	• Attacking wrong target if coordination not made with EW	• Should be no conflict
Counterpropaganda can conflict by	• Revealing information to counter adversary PSYOP	• If the deception story does not agree with counterpropaganda information	• Taking away assets normally devoted to projecting PSYOP themes	• Friendly fratricide can be used as propaganda by enemy	• Targeting sources needed to receive counterpropaganda	• Should be no conflict
CI can conflict by	• Should be no conflict	• Should be no conflict	• Should be no conflict	• Killing sources	• ES may be needed for other activities	• Should be no conflict

Figure 2-2. Potential Conflicts within the Elements of IO (continued)

	IA	Counterdeception	Counterpropaganda	CI	CNA	CND
Counterdeception can conflict by	• By allowing enemy misinformation to cause repudiation of friendly information		• If information needed to influence the deception target is inconsistent with information needed to influence populace	• CI assets are not used in counterdeception actions	• Should be no conflict	• Should be no conflict
Counterpropaganda can conflict by	• Should be no conflict	• If counterdeception attempts to exploit the enemy's deception are not synchonized with counterpropaganda attempts to counter the enemy's message		• CI and counterpropaganda may be directed toward one target but with opposite effects. CI tries to get to the intelligence source; CP tries to counter distorted messages from the source	• Attack of wrong target with CNA can be used as enemy propaganda	• Should be no conflict
CI can conflict by	• Ineffective CI can negate information integrity	• Ineffective CI prevents negating counterdeception	• Ineffective CI does not nullify enemy propaganda		• Should be no conflict	• CI revealing how networks are protected

Figure 2-2. Potential Conflicts within the Elements of IO (continued)

	IO	CMO	PA
IO supports by		• Influencing/informing populace of CMO activities and support • Neutralizing misinformation and hostile propaganda directed against civil authorities • Controlling electromagnetic spectrum for legitimate purposes	• Conducting counterpropaganda and protection from misinformation/rumor • Developing EEFI to preclude inadvertent public disclosure • Synchronizing PSYOP and OPSEC with PA strategy
CMO supports by	• Providing information to support friendly knowledge of information environment • Synchronizing communications media and message with PSYOP • Coordinating C2 target sets with targeting cell • Establishing and maintaining liaison or dialogue with indigenous personnel and NGOs • Supporting PSYOP with feed back on PSYOP themes • Providing news and information to the local people		• Providing information on CMOC activities to support PA strategy • Synchronizing information communications media and message • Identifying, coordinating, and integrating media, public information, and host-nation support
PA supports by	• Developing information products to protect soldiers against the effects of misinformation or disinformation • Coordinating with PSYOP and counterpropaganda planners to ensure a consistent message and maintain OPSEC • Support counterpropaganda by countering misinformation • Providing assessment of effects of media coverage to OPSEC planners • Providing assessment of essential nonmedia coverage of deception story	• Producing accurate, timely, and balanced information for the public • Coordinating with CA specialists to verify facts and validity of information	

Figure 2-3. Support Roles of IO, Civil Military Operations, and Public Affairs

Chapter 3

Operations Security

Operations security (OPSEC) is the process commanders and staffs follow to identify and protect essential elements of friendly information. Units and soldiers implement OPSEC measures as part of force protection. OPSEC is not a *collection* of specific measures to apply to every operation. It is a *methodology* that applies to any operation or activity at all levels of command. This chapter establishes Army OPSEC doctrine and TTP. First, it explains the OPSEC process established in JP 3-54. Then it describes how commanders and staffs apply it to the military decisionmaking process and other operations process activities.

OPERATIONS SECURITY AND INFORMATION OPERATIONS

3-1. ***Operations security is*** **a process of identifying essential elements of friendly information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive essential elements of friendly 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.** Operations security (OPSEC) applies across the range of Army operations and spectrum of conflict. All units—combat, combat support, and combat service support—conduct (plan, prepare, execute and assess) OPSEC operations to preserve essential secrecy. OPSEC has a reputation of being little more than performing trivial tasks; however, it is vital to success in all types of operations. Often what information friendly forces take for granted is what adversaries need to defeat them. Execution of effective OPSEC measures (see definition paragraph 3-15), however routine, denies adversaries this information and increases the effectiveness of friendly forces.

CONTENTS

3-2. All soldiers execute OPSEC measures. These cover a range of activities, from maintaining silence among peers and family to camouflaging equipment. Effective OPSEC requires disseminating OPSEC guidance to every soldier. Good OPSEC involves telling soldiers why OPSEC measures are important and what they are supposed to accomplish. All must understand the cost of failing to maintain effective OPSEC. Understanding why they are doing something and what their actions are supposed to accomplish, allows soldiers to execute tasks more effectively. Active and deliberate actions by individual soldiers are critical to successful OPSEC.

THE OPERATIONS SECURITY PROCESS

3-3. Army forces follow the OPSEC process prescribed in JP 3-54. As with other processes, such as targeting and intelligence preparation of the battlefield (IPB), commanders synchronize OPSEC planning during the military decision-making process (MDMP). The OPSEC process includes five actions that apply to any operation. They provide a framework to systematically identify, analyze, and protect essential elements of friendly information (EEFI). The OPSEC process is continuous. G-7s use it to assess the changing nature of adversary operations and friendly vulnerabilities throughout an operation. The OPSEC process is conducted by the OPSEC officer. Actions that compose the OPSEC process follow a sequence. However, as with the MDMP, staffs avoid following the sequence lockstep. Information affecting an OPSEC action can arrive at any time. Effective staffs process the information, enter the OPSEC process at the appropriate point, and execute the actions necessary to act on the information. The following paragraphs discuss the OPSEC actions in the order they logically occur.

OPSEC Process Actions

- Identification of EEFI
- Analysis of adversaries
- Analysis of vulnerabilities
- Assessment of risk
- Application of appropriate OPSEC measures

OPSEC ACTION 1 – IDENTIFICATION OF ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

3-4. The product of this OPSEC action is EEFI, a list of information that needs protection. The Army defines *essential elements of friendly information* as the critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation, and therefore must be protected from detection (FM 3-0). Army doctrine defines EEFI differently from joint doctrine. The joint definition of EEFI focuses on information adversaries want to collect. The Army definition focuses on information friendly commanders want to protect. The joint definition of EEFI includes friendly information that may not compromise friendly operations. However, collecting it consumes resources that adversaries could use to collect EEFI. Army OPSEC doctrine addresses protecting information that is relevant from the adversary's perspective. It does not address what joint doctrine considers EEFI.

3-5. The OPSEC process begins with the commander's initial guidance during receipt of mission. The G-7 recommends initial EEFI if the commander

does not name any in the initial guidance. Several sources help G-7s determine information to recommend as EEFI:

- The commander's guidance.
- The IO estimate.
- The OPSEC estimate (provided by the OPSEC officer and coordinated with the G-7).
- The intelligence estimate (information about the adversary and adversary intelligence requirements).
- The multidiscipline counterintelligence estimate (normally an appendix to annex B to the operation order (OPORD) or operation plan (OPLAN), or a tab to the intelligence estimate).
- The higher headquarters security classification guide for the operation. The security classification guide identifies classified information and EEFI related to the operation. It is itself sensitive information since it names, by classification level, the operation's most sensitive areas.
- Laws and executive orders that require protection of unclassified controlled information.
- The multidiscipline counterintelligence section of the G-2 analysis and control element (ACE).

3-6. Commanders determine EEFI. Staffs determine OPSEC measures to shield EEFI from adversary collection systems. EEFI are not part of the commander's critical information requirements (CCIR); however, they become priorities when commanders establish them.

3-7. The staff identifies possible EEFI and recommends them to the commander throughout the MDMP. Facts, assumptions, and essential tasks may reveal EEFI that apply to the operation. In addition, each course of action (COA) may have EEFI that apply only to it. As the staff war-games a COA, the G-2 identifies friendly information that, if known to adversaries, would allow them to counter the COA. The G-7 adds these elements of information to the EEFI for that COA, recording them in the IO estimate (see appendix C). Upon COA approval, the EEFI for the approved COA becomes the EEFI for the operation.

3-8. When identifying EEFI, the G-7 determines the period during which each EEFI element needs protection. Not all EEFI need protection throughout an operation. Some elements need to be protected only during specific events; others may not need protection until a branch or sequel is executed.

OPSEC ACTION 2 – ANALYSIS OF ADVERSARIES

3-9. The purpose of this OPSEC task is to identify the adversary's most dangerous and most probable use of collection assets. This analysis focuses on the EEFI. The most dangerous situation is one in which an adversary has the intelligence, surveillance, and reconnaissance (ISR) assets needed to collect data from friendly OPSEC indicators and determine the EEFI. The most likely situation is based on how the adversary has used his assets during past operations. The G-2, G-3, G-7, and OPSEC officer perform this action as part of IPB. Adversary intentions and collection capabilities are identified with the help of these questions:

- Who are the adversaries?
- Who has the intent and capabilities to act against the planned operation?
- What are probable adversary objectives?
- What are likely adversary actions against friendly operations?
- What information do adversaries already know?
- What collection capabilities do adversaries possess or have access to by financial arrangement or shared ideologies, or coordinated coalitions/ alliances?
- Which OPSEC indicators can be faked to deceive adversaries?

OPSEC ACTION 3 – ANALYSIS OF VULNERABILITIES

3-10. This OPSEC action determines OPSEC vulnerabilities of an operation or activity. It has two steps:

- Identify OPSEC indicators.
- Identify OPSEC vulnerabilities.

3-11. *Operations security indicators* are friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive essential elements of friendly information. (The joint and Army definitions are similar. The Army definition substitutes *EEFI* for *critical information*.) The G-2, G-3, G-7, and OPSEC officer examine all aspects and phases of the operation to find OPSEC indicators. They then compare them with the adversary targeting cycle and collection capabilities, considering these questions:

- What OPSEC indicators will friendly forces create during the operation?
- What OPSEC indicators can the adversary actually collect?
- What OPSEC indicators will the adversary be able to use to the disadvantage of friendly forces?

The answer to the last question is OPSEC vulnerabilities.

3-12. An *operations security vulnerability* is a condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decisionmaking (JP 1-02). An OPSEC vulnerability exists when an adversary can collect information from an OPSEC indicator, correctly analyze the information, make a decision, and take timely action to degrade friendly operations or place itself in an advantage over friendly forces.

3-13. Analysis of OPSEC vulnerabilities begins during mission analysis and continues through COA development. COA analysis, and assessments during preparation and execution may also identify OPSEC vulnerabilities. Field support teams from the 1st Information Operations Command (Land) (1st IOC [L]), formerly known as the Land Information Warfare Activity (LIWA), can assist in this effort (see appendix F). The G-7 and OPSEC officer record OPSEC vulnerabilities and analyzes them further during the next OPSEC action, assessment of risk.

OPSEC ACTION 4 – ASSESSMENT OF RISK

3-14. The staff assesses risks associated with the overall operation during mission analysis and COA development (see chapter 5 and appendix B). The G-7 and OPSEC officer assess the risks posed by OPSEC vulnerabilities concurrently. The purpose of this OPSEC assessment of risk is to select OPSEC measures that shield OPSEC vulnerabilities and require the fewest resources. This OPSEC action has four steps:

- Conduct a risk assessment for each OPSEC vulnerability.
- Select one or more OPSEC measures for each OPSEC vulnerability.
- Determine residual risk for each OPSEC vulnerability.
- Decide which OPSEC measures to implement.

3-15. ***Operations security measures*** **are methods and means to gain and maintain essential secrecy about essential elements of friendly information**. (The joint and Army definitions of OPSEC measures are similar. The Army definition substitutes *EEFI* for *critical information.* The joint definition also includes the OPSEC measure categories.) The following categories apply:

- **Action control**. The objective of action control is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake; decide whether to execute actions; and determine the "who," "when," "where," and "how" for actions necessary to accomplish tasks.
- **Countermeasures**. The objective of countermeasures is to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering and processing capabilities.
- **Counteranalysis**. The objective of counteranalysis is to prevent accurate interpretations of indicators during adversary analysis of collected materials. Confusing the adversary analyst through deception techniques such as cover does this.

The most desirable OPSEC measures provide the needed protection at least cost to operational effectiveness.

3-16. The OPSEC officer begins assessment of risk by analyzing the OPSEC vulnerabilities identified in the previous OPSEC actions and identifying possible OPSEC measures for each one. Some OPSEC measures may protect more than one OPSEC vulnerability. As part of this step, the OPSEC officer evaluates the sufficiency of standard security measures. This evaluation covers such areas as personnel, physical, cryptographic, document, special access, and automated information systems (INFOSYS) security. It may include an OPSEC review. Continuing OPSEC measures in these areas may provide the necessary protection for some OPSEC vulnerabilities.

3-17. The OPSEC officer then determines the residual risk for each OPSEC vulnerability after the appropriate OPSEC measures are applied to it. The OPSEC officer uses the procedure described in paragraphs B-14–B-17 (see FM 100-14 for a full explanation.) *Residual risk* is the level of risk remaining after controls have been identified and selected for hazards that may result

in loss of combat power (FM 100-14). In this context, OPSEC measures are controls.

3-18. Finally, the OPSEC officer selects OPSEC measures to recommend based on this assessment of risk. The G-7 compares the residual risk with the risk posed by the OPSEC vulnerability if the OPSEC measure is not executed. The difference allows the G-7 to estimate the benefit gained from the OPSEC measure. In deciding which OPSEC measures to recommend, the OPSEC officer considers the following questions:

- What is the cost in terms of combat power if an OPSEC measure is employed? Does the cost jeopardize mission success? The OPSEC officer may recommend a no-measures alternative if cost outweighs the risk.
- What is the risk to mission success if an OPSEC measure is not executed?
- What is the risk to mission success if an OPSEC measure fails?

3-19. The OPSEC officer coordinates proposed OPSEC measures across the staff to minimize redundancy and ensure they do not create new OPSEC indicators. The OPSEC double-checks these factors during COA analysis.

OPSEC ACTION 5 – APPLICATION OF APPROPRIATE OPSEC MEASURES

3-20. The G-7 recommends OPSEC measures to the G-3. These may include OPSEC measures that entail significant expenditures of time, resources, or personnel. Commanders normally approve OPSEC measures during COA approval. Approved OPSEC measures become OPSEC tasks. The G-7 determines criteria of success for them, ensures the OPLAN/OPORD includes them, and makes the arrangements necessary to assess them throughout preparation and execution (see chapter 5). The G-3 directs execution of OPSEC measures in warning orders (WARNOs) or fragmentary orders (FRAGOs).

3-21. Once the commander approves OPSEC measures, the OPSEC officer monitors their implementation and evaluates them in terms of their criteria of success. The OPSEC officer adjusts measures, if necessary, based on this assessment. The OPSEC officer coordinates monitoring of OPSEC measures with the G-2 and counterintelligence staffs to ensure it receives the appropriate priority. Monitoring may generate IO information requests (IRs). The OPSEC officer passes these to the G-2 for inclusion in the collection plan. Some of these IO IRs may become priority information requirements (PIRs).

3-22. Maintaining OPSEC is a continuous requirement. Assessing OPSEC measures includes collecting lessons learned. Most lessons arise while monitoring execution of OPSEC measures (OPSEC assessments). Others arise from an evaluation of a completed operation or program (OPSEC checks).

CONDUCTING OPSEC OPERATIONS

3-23. The G-7, assisted by the OPSEC officer, helps the G-3 integrate OPSEC into the operations process by combining the OPSEC process with risk management (see FM 100-14). *Risk management* is a process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits, (JP 1-02). Commanders use it to conserve combat power and resources by identifying and controlling hazards.

(A *hazard* is a condition with the potential to cause injury, illness, or death of personnel; damage to, or loss of, equipment or property; or mission degradation [FM 100-14].) Risk management is an integral part of the MDMP.

3-24. An OPSEC vulnerability is a type of hazard related to EEFI. Unprotected OPSEC vulnerabilities entail tactical risk. (*Tactical risk* is risk associated with hazards that exist due to the presence of adversaries. *Accident risk* includes all operational risk considerations other than tactical risk [FM 100-14]. The OPSEC process addresses only tactical risk.) Because it is used to assess all types of risk, risk management allows the OPSEC officer to integrate assessments of risks from OPSEC vulnerabilities with assessments of other-IO related risks. Figure 3-1 shows the relationship of the steps of the risk management process, the actions of the OPSEC process, and the activities of the operations process.

	Operations Process Activity	OPSEC Action	Risk Management Step
ASSESSMENT	PLANNING	• Identify EEFI • Analysis of adversaries • Analysis of vulnerabilities	• Identify hazards
		• Assessment of risk	• Assess hazards • Develop controls and make risk decisions
	PREPARATION EXECUTION	• Application of appropriate OPSEC measures	• Implement controls
	ASSESSMENT		• Supervise and evaluate

Figure 3-1. Integration of the Operations, Risk Management, and OPSEC Processes

3-25. Commanders conduct OPSEC operations to protect EEFI, a defensive IO objective. The product of OPSEC planning is a set of coordinated OPSEC measures that soldiers and units execute to protect the force. Throughout the MDMP, the G-7 treats OPSEC measures as IO tasks. During orders production, the G-7 incorporates OPSEC measures throughout the OPLAN/OPORD as IO tasks and tasks to subordinate units.

PLANNING

3-26. The OPSEC officer performs OPSEC actions throughout the MDMP.

- During receipt of mission, mission analysis, and COA development, the OPSEC officer identifies OPSEC vulnerabilities (OPSEC-related hazards) and assesses the risks they pose.
- During COA analysis, the OPSEC officer tests the OPSEC measures (controls) associated with each COA by analyzing OPSEC measures from the adversary perspective.
- During COA comparison, the OPSEC officer determines which OPSEC measures to recommend for each COA and which COA is most supportable from an OPSEC perspective.

- During COA approval, the OPSEC officer recommends OPSEC measures to counter the risks posed by OPSEC vulnerabilities. The commander decides which OPSEC measures to implement.
- During orders production, the OPSEC officer follows up on coordination done during the MDMP and ensures the OPLAN/OPORD contains instructions necessary to prepare, execute, and assess the approved OPSEC measures.

3-27. The IO estimate is the OPSEC officer's primary source of OPSEC-related information (see appendix C). The G-7 updates it continuously throughout the operation based on input from IO cell representatives. In a time-constrained environment, a current IO estimate may be the only readily available source of OPSEC-related information. The IO estimate contains the following:

- The probable adversary picture of friendly forces (paragraph 2a[4], IO estimate).
- Adversary collection capabilities (paragraph 2b[3], IO estimate).
- The current EEFI (paragraph 2d[1], IO estimate).
- OPSEC indicators (paragraph 2d[2], IO estimate).
- OPSEC measures in effect (paragraph 2d[3], IO estimate).
- OPSEC measures contemplated (paragraph 2d[4], IO estimate).

Receipt of Mission

3-28. During receipt of mission, the OPSEC officer starts the following OPSEC actions:

- Identify EEFI.
- Analyze adversaries.

The OPSEC products for receipt of mission are a list of initial EEFI, and a list of OPSEC-related input to the initial ISR tasking.

3-29. **Identify Essential Elements of Friendly Information**. The commander's initial assessment and commander's initial guidance may result in initial EEFI or guidance on developing them. If the commander does not establish initial EEFI, the G-7 recommends initial EEFI based on the IO estimate and initial IO assessment. The G-3 disseminates the initial EEFI in the initial warning order if they are different from the EEFI for the current operation. Paragraph 2d of the IO estimate lists approved EEFI.

3-30. **Analyze Adversaries**. The G-7 provides the initial EEFI to the G-2 for consideration in the initial IPB. IO IRs concerning adversary capability to collect EEFI are submitted to the G-2 for inclusion in the initial ISR tasking.

Mission Analysis

3-31. The G-7s related product of mission analysis is the OPSEC planning guidance. It is normally part of the commander's guidance and included in the WARNO that disseminates it.

3-32. ***Operations security planning guidance*** **serves as the blueprint for operations security planning. It defines the essential elements of friendly information, taking into account friendly and adversary**

goals, probable adversary knowledge, friendly deception objectives, and adversary collection capabilities. It also should outline provisional operations security measures. (The joint and Army definitions for OPSEC security planning guidance are different. The Army definition substitutes EEFI for critical information, a joint term that the Army does not use. It does not refer to estimated key adversary questions because these cannot be determined with any certainty. It deletes desirable adversary appreciations and harmful adversary appreciations because these are no longer defined joint terms; it replaces them with deception objectives to link OPSEC and deception planning. It replaces pertinent intelligence system threats with adversary collection capabilities for clarity.)

3-33. The G-7 develops the OPSEC planning guidance by—

- Continuing to identify EEFI.
- Continuing the analysis of adversaries.
- Beginning the analysis of vulnerabilities
- Beginning the assessment of risk.

3-34. **Identify Essential Elements of Friendly Information**. The G-7 identifies additional EEFI and reviews and refines existing EEFI throughout mission analysis, based on input from IO cell representatives. MDMP tasks that may yield additional EEFI are—

- Conduct IPB.
- Determine specified, implied, and essential tasks.

3-35. IO cell members consider friendly and adversary goals, probable adversary knowledge, friendly deception objectives, and adversary collection capabilities when developing additional EEFI.

3-36. **Analyze Adversaries**. The OPSEC officer participates in IPB throughout the operation to determine the adversary's most dangerous and most likely use of collection assets.

3-37. **Analysis of Vulnerabilities and Assessment of Risk**. OPSEC indicators are possible OPSEC-related hazards. During the MDMP task *conduct risk assessment*, OPSEC indicators are identified at the same time as hazards associated with IO tasks. The 1st IOC (L) field support teams can support this effort. They provide support to land component and Army commands to facilitate the conduct of IO. Additionally, they enhance worldwide force protection by carrying out a proactive defense of Army information and INFOSYS. The OPSEC officer then assesses the risks associated with those hazards before controls (including OPSEC measures) are applied to mitigate the risk. This assessment allows the OPSEC officer to determine whether any identified OPSEC indicators result in OPSEC vulnerabilities. Sources of information that contribute to this determination are—

- The ongoing IPB.
- Critical facts and assumptions, particularly assumptions made to replace missing or unknown OPSEC-related facts.
- Constraints that affect possible OPSEC measures.

The OPSEC officer establishes provisional OPSEC measures to shield any OPSEC vulnerabilities and determines residual risk (see figure B-10, page B-14).

These provisional OPSEC measures and any changes to the initial EEFI constitute the OPSEC planning guidance, which is disseminated in a WARNO after command approval. The residual risk figures give commanders a tool to help decide how to allocate resources associated with OPSEC measures and where to accept risk, if necessary.

Course of Action Development

3-38. During COA development, the G-7 —

- Continues to identify EEFI.
- Continues analysis of adversaries.
- Continues analysis of vulnerabilities.
- Continues assessment of risk.

The OPSEC products for COA development are, for each COA, additional EEFI, OPSEC vulnerabilities, OPSEC measures, and the residual risk associated with each OPSEC vulnerability.

3-39. **Identify Essential Elements of Friendly Information**. During mission analysis, the G-7 identified EEFI associated with the overall operation. During COA development, the G-7 identifies additional EEFI associated with each COA and with the critical asset list (see paragraph 5-46). These EEFI are not disseminated unless the G-7 determines that they affect the success of the operation regardless of which COA the commander approves.

3-40. **Analysis of Adversaries**. The OPSEC officer continues to participate in IPB. The OPSEC officer contributes information IO cell developed by the and obtains the most current information on adversary capabilities and intentions.

3-41. **Analysis of Vulnerabilities and Assessment of Risk**. As each COA is developed, the OPSEC officer identifies OPSEC indicators and assesses them to determine whether any constitute OPSEC vulnerabilities (hazards). 1st IOC (L) field support teams can assist in this effort. The OPSEC officer develops OPSEC measures (controls) for all OPSEC vulnerabilities and determines the residual risk associated with each OPSEC vulnerability. This information is recorded on the G-7 risk management worksheet (see figure B-10, page B-14). The OPSEC officer considers measures to counter OPSEC vulnerabilities in the following areas:

- Operational.
- Logistic.
- Technical.
- Administrative.
- Military deception.
- Physical destruction.
- Electronic warfare.
- Public Affairs (PA).
- Civil Military Operations.

3-42. The OPSEC officer coordinates OPSEC measures as they are developed. Coordination may include developing rules of engagement for some OPSEC measures. Coordination requirements may include—

- Determining the effects of some OPSEC measures on PA operations.
- Obtaining guidance on terminating OPSEC measures.
- Obtaining guidance on declassification and public release of OPSEC-related activities.
- Obtaining administrative and logistic support for OPSEC tasks.
- Establishing OPSEC coordination measures and command and control measures.
- Establishing assessment (monitoring and evaluation) mechanisms.
- Submitting IO IRs and requests for information to support assessment of IO tasks.
- Conducting OPSEC checks.
- Arranging input for after-action reports.
- Arranging support of OPSEC-related communications requirements.

Course of Action Analysis (War-gaming)

3-43. COA analysis allows the OPSEC officer to test OPSEC measures associated with each COA. During the war game, the commander may modify the COA based on how events develop. The OPSEC officer determines whether modifications result in additional EEFI or OPSEC vulnerabilities. If so, the OPSEC officer recommends OPSEC measures to shield them. In addition, the G-7—

- Continues to identify EEFI.
- Continues analysis of adversaries.
- Continues analysis of vulnerabilities.
- Continues assessment of risk.

3-44. The OPSEC products for COA analysis are, for each COA, an evaluation in terms of criteria established before the war game and refined lists of EEFI, OPSEC vulnerabilities, and OPSEC measures. The OPSEC officer also determines—

- Decision points for executing OPSEC measures.
- Operational support needed for OPSEC measures.
- OPSEC measures needed to support possible OPSEC branches and sequels.
- Whether any OPSEC measures require addition coordination.

3-45. **Identify Essential Elements of Friendly Information**. The G-7 records any additional EEFI revealed during the war game, particularly those that result from modifying a COA. The OPSEC officer determines whether they produce OPSEC indicators.

3-46. **Analysis of Adversaries and Analysis of Vulnerabilities**. The OPSEC officer notes additional adversary capabilities; additional OPSEC indicators, including OPSEC indicators produced by newly identified EEFI; and any gaps in the IPB revealed during the war game. The OPSEC officer determines whether adversary capabilities and OPSEC indicators revealed during the war game result in OPSEC vulnerabilities. If so, the OPSEC officer develops OPSEC measures to shield them. The OPSEC officer works with the G-2 to obtain information to fill IPB gaps.

3-47. **Assessment of Risk**. The OPSEC officer determines criteria for comparing COAs from an OPSEC perspective before beginning the war game. During the war game, the OPSEC officer evaluates the effectiveness of each OPSEC measure. The OPSEC officer also assesses the residual risk associated with any IO vulnerabilities identified during the war game, determines appropriate IO measures, and tests them.

3-48. **Evaluation of Courses of Action**. After war-gaming each COA, the OPSEC officer evaluates it based on criteria established before beginning the war game. The OPSEC officer also identifies each COA's strengths, weaknesses, advantages, and disadvantages. Criteria include costs associate with OPSEC measures and the risk involved with implementing or not implementing them.

Course of Action Comparison

3-49. During COA comparison, the staff compares feasible COAs to identify the one with the highest probability of success against the most likely adversary COA and the most dangerous adversary COA. The G-7 product of COA comparison is a determination of which COA is most supportable in terms of IO. That determination is included in the staff recommendation to the commander during COA approval. The G-7 considers all IO elements when comparing COAs, not just OPSEC. The G-7 makes this determination based on the comparison criteria established before the war game.

3-50. During COA comparison, the OPSEC officer completes OPSEC action 4, assessment of risk, by determining which IO measures (controls) to recommend for each COA (recommending a risk decision). The G-7 considers the costs associated with these measures when recommending a COA for command approval.

Course of Action Approval

3-51. During COA approval, the staff recommends a COA to the commander for execution. The recommended COA includes OPSEC measures identified and tested during the preceding MDMP tasks. The OPSEC officer identifies OPSEC measures that entail significant resource expenditure or risk and requests decisions concerning them. Otherwise, when the commander approves a COA, he approves the OPSEC measures associated with it.

Orders Production

3-52. During orders production, the OPSEC officer follows up on coordination done during the MDMP. The OPSEC officer—

- Ensures the OPLAN/OPORD contains the instructions necessary to prepare, execute, and assess approved OPSEC measures.
- Prepares the OPSEC paragraph of the IO annex and the OPSEC appendix to the IO annex.
- Ensures all concerned know which OPSEC measures are approved.

3-53. During orders production, G-7—

- Follows up on coordination done during COA development.
- Ensures EEFI are listed in the OPLAN/OPORD coordinating instructions.

- Ensures OPSEC measures (IO tasks) are included in the tasks assigned to subordinate units.

PREPARATION AND EXECUTION

3-54. During preparation and execution, the G-7 monitors and evaluates preparation and execution of all IO tasks. These actions include overseeing application of OPSEC measures for the approved COA (supervising the implementation of controls). The OPSEC officer—

- Assesses (monitors and evaluates) execution of OPSEC measures.
- Recommends/directs OPSEC measure changes based on assessments. These changes are normally directed by the FRAGO.

ASSESSMENT

3-55. Monitoring and evaluating OPSEC measures are continuous throughout the OPSEC process. IO cell members are alert for any OPSEC indicators in their functional areas that may result in OPSEC vulnerabilities. The preceding paragraphs have noted how continuous assessment contributes to refining OPSEC products. They also identified places where 1st IOC (L), field support teams can assist in this effort.

3-56. Commanders use the following tools to assess OPSEC:

- OPSEC review.
- OPSEC assessment.
- OPSEC check.

OPSEC reviews are addressed in most units standing operating procedures. An OPSEC review is an example of an OPSEC measure that is routine, but important. OPSEC assessments and OPSEC checks are more elaborate and resource intensive. Commanders use them based on the situation, primarily the time and resources available. Figure 3-2 contains examples of questions OPSEC officers can ask to determine the status of OPSEC in the command.

• Time interval since subordinate commanders have changed their daily movement plans. • Frequency of friendly attack patterns repeated consecutively. • Number of elements of EEFI covered by two or more OPSEC measures. • Number of collection efforts against EEFI. • Vulnerability of the friendly plan, determined from self-monitoring of EEFI. • Number of friendly OPSEC vulnerabilities exploited by adversary action. • Number of friendly operations disrupted by adversary detection and response. • Number of support facilities protected from adversary observation.	• Number of friendly operational movements conducted outside adversary overhead surveillance. • Frequency of coordination between OPSEC and deception planners. • Number of OPSEC measures selected based on the vulnerability analysis. • Number of times OPSEC planners have had access to compartmented planning efforts. • Number of times OPSEC guidance has been received from higher headquarters. • Percent of routine actions with timing or location changed at least weekly. • Number of units equipped with antisurveillance sensor and sensor jamming devices.

Figure 3-2. OPSEC Status Indicators

OPSEC Review

3-57. All staff sections review staff documents and INFOSYS logs to ensure protection of sensitive information. Standing operating procedures should state which documents (for example, news releases) automatically go to the OPSEC officer for review. They should also provide standards for protecting, storing, and handling sensitive information and INFOSYS. When corrective action is necessary, such as an OPSEC assessment or review, the OPSEC officer provides recommendations to the appropriate staff officer.

OPSEC Assessment

3-58. OPSEC assessments monitor an operation to determine the unit's overall OPSEC posture and evaluate compliance of subordinate organizations with the OPSEC appendix to the IO annex. OPSEC officers conduct OPSEC assessments. They submit results and recommendations to the commander.

OPSEC Check

3-59. The OPSEC officer conducts, with appropriate assistance, OPSEC checks. An OPSEC check determines if the command is adequately protecting EEFI. It analyzes the conduct of the operation to identify sources of OPSEC indicators, what they disclose, and what can be learned from them. The objective is to identify unprotected OPSEC vulnerabilities. OPSEC checks help commanders assess OPSEC measures and adjust them if necessary. Effective OPSEC checks require careful planning, thorough data collection, and thoughtful analysis. They are resource intensive, so the OPSEC officer usually executes an informal assessment first to determine if there is a need for a complete OPSEC check.

3-60. An OPSEC check attempts to reproduce the intelligence image that a specific operation projects. From that image, the OPSEC officer identifies OPSEC vulnerabilities. OPSEC checks differ from adversary collection efforts in that they occur within a limited period and normally do not use covert means. They verify the existence of OPSEC indicators by examining all of an organization's functions at all points of the operations process. An OPSEC check traces the flow of information from start to finish for each function.

3-61. OPSEC checks vary based on the nature of the information being protected, the adversary collection capability, and the environment. In combat, they identify actual OPSEC vulnerabilities. In peacetime, they identify potential OPSEC vulnerabilities.

3-62. OPSEC checks should not be conducted as inspections. There is no grade and there is no report to the checked unit's higher headquarters. An OPSEC check should not focus on the effectiveness of security programs or adherence to security directives. Such compliance-based evaluations should be conducted as inspections.

Chapter 4

Military Deception

This chapter establishes Army doctrine and tactics, techniques, and procedures for military deception. Section I discusses the forms and principles of military deception. It also states how military deception supports each type of military operation. Section II describes how to conduct (plan, prepare, execute, and assess) military deception operations in terms of the operations process and military decisionmaking process.

SECTION I – MILITARY DECEPTION DOCTRINE

4-1. *Military deception* comprises those actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (JP 3-58; the complete joint definition includes the five categories of military deception [MD] operations listed in figure 4-1, page 4-3). It is often the key to achieving surprise and can enable a force to achieve its objectives while minimizing losses and maximizing tempo. Skillfully applied, MD can significantly enhance the likelihood of success, contribute to economy of force, and reduce friendly casualties.

4-2. Adversary decisionmakers are the overall target of MD; however not all adversaries are military, and commanders may also want to deceive others who are not adversary host-nation civilians. Such actions are taken to protect the force.

CONTENTS

4-3. Opportunities to use MD occur in most military operations. Commanders may use MD to establish conditions favorable to success while preparing to deploy. Once deployed, commanders can tailor deception objectives to support each phase of an operation. The probability of success increases when commanders consider it early in the military decisionmaking process (MDMP).

4-4. A part of both offensive and defensive information operations (IO), MD is a fundamental instrument of military art. Its ultimate goal is to deceive adversaries and others about friendly force dispositions, capabilities, vulnerabilities, and intentions. MD supports achieving the commander's intent by—

- Disrupting the adversary's ability to synchronize operations.
- Causing adversaries to hesitate in making decisions.
- Seizing, retaining, and exploiting the initiative.
- Reducing the conflict's intensity.
- Damaging the adversary's will to fight.
- Directing adversary intelligence, surveillance, and reconnaissance (ISR) operations away from friendly operations.
- Increasing the adversary's uncertainty (fog of war).

4-5. MD also helps protect the force from adversary offensive IO. MD efforts mislead adversaries about friendly command and control (C2) capabilities and vulnerabilities and delay decisions due to confusion from the fog of war. Successful MD may cause adversaries to misallocate resources.

4-6. While the general concepts and basic principles of MD are ageless, new technologies allow targeting of adversary decisionmakers throughout the area of operations (AO). The combined effects of the following post-Cold-War trends are creating new opportunities and challenges for conducting MD operations:

- Integration of IO into all operations.
- Expanding range of missions.
- Joint and multinational nature of missions.
- Accelerating tempo.
- Relatively short mission duration.
- Growing sophistication, connectivity, and reliance on information technology, digitized technologies, and automated C2 systems.

4-7. FM 6-0 lists the responsibilities of coordinating and special staff officers. The MD responsibilities of commanders and staffs parallel those in other types of military operations. Commanders provide direction throughout MD operations. They ensure that MD plans and execution conform to statutory requirements, international agreements, and any instructions from higher headquarters.

4-8. Intelligence activities support MD. Intelligence support provides insights into the deception target's vulnerabilities, beliefs, and access. It also provides details from the adversary's perspective to make the deception believable to the deception target. Intelligence support monitors a variety of indicators—collected against priority intelligence requirements (PIRs)— to determine how the adversary is responding to the deception.

CATEGORIES OF MILITARY DECEPTION

4-9. Joint doctrine establishes the five categories of MD shown in figure 4-1 (see JP 3-58). The Army doctrinal hierarchy categorizes IO as a type of enabling operation. MD is an element of IO.

Category	Objective	Characteristics
Strategic Military Deception	• Results in adversary military policies and actions that support the originator's strategic military objectives, policies and operations	• Conducted by and in support of senior military commanders
Service Military Deception	• Designed to protect and enhance the combat capabilities of Service forces and systems • Protects friendly force personnel, materiel, equipment, and INFOSYS nodes from observation and surveillance using natural or artificial material	• Conducted by the Services that pertains to service support to joint operations • Imitates, in any sense, a person, object, or phenomenon to deceive adversary surveillance devices or mislead adversary evaluation • Targets sensors and weapon systems • Employed against systems
Operational Military Deception	• Results in adversary actions favorable to the originator's objectives and operations • For Army forces, a subcategory of Service military deception	• Conducted in a theater of war to support campaigns and major operations
Tactical Military Deception	• Influence an adversary commander to act in a manner that serves US tactical objectives • For Army forces, a subcategory of Service military deception	• Targets adversary decisionmakers at any level of command • Supports battles and engagements • Integral to the concept of operations • Requires feedback planning • Centrally monitored and controlled
Military Deception in Support of OPSEC	• Degrades adversary capability to discern OPSEC vulnerabilities	• Targets adversary intelligence functions • Employed against all forms of ISR operations • Supports force protection • Derived from the concept of operations • Feedback not always required • Decentralized control and execution

Figure 4-1. Categories of Military Deception Operations

4-10. Army doctrine considers operational and tactical MD to be part of Service MD. From the perspective of a joint force headquarters, Army forces conduct Service MD operations. From the Army force perspective, the echelon planning an MD operation determines its type: Corps and echelons above corps conduct operational MD operations; division and lower headquarters conduct tactical MD operations. Army forces do not plan strategic MD operations. However, Army forces may participate in executing them.

PRINCIPLES OF MILITARY DECEPTION

4-11. Following the principles of MD contributes to successful MD operations. Applying them consistently and creatively enhances any deception's credibility and increases its chances for success. However, they are not a checklist that guarantees success. Commanders and staffs use judgment to apply them.

FOCUS ON THE TARGET

4-12. MD operations focus on a deception target. The *deception target* is the adversary decisionmaker with the authority to make the decision that will achieve the deception objective (JP 3-58). (See definition of deception objective in paragraph 4-15.) For example, an MD operation designed to delay the movement of an adversary reserve would target the commander who could make the decision to commit it. The adversary's intelligence system is the channel for getting the deception story to the deception target. It is not normally the target itself.

4-13. The more that is known about the deception target, the greater the effect that can be achieved and the better the chances of success. The target's assessment and decision-making processes are the main elements against which an MD operation operates. Understanding how the adversary C2 system collects, processes, and disseminates information from the collector to the target allows injection of *indicators* (see definition, paragraph 4-20) at the proper places and times to create the *desired perceptions* (see definition, paragraph 4-36). Also useful is detailed knowledge of the target's biases, for example, how the target reacts to various kinds of messages, and which information sources the target finds most reliable.

Principles of Military Deception

- Focus on the target
- Cause the target to act
- Centralize control
- Employ variety
- Enforce strict OPSEC
- Minimize falsehood/leverage truth
- Ensure timeliness
- Ensure integration
- Exploit target biases
- Avoid windfalls
- Utilize space effectively
- Work within available competencies and resources

CAUSE TARGET TO ACT

4-14. An effective MD operation leads the deception target to take (or not take) specific actions that favor friendly force operations. The situation that the commander wants to create by these actions is the deception objective.

4-15. A *deception objective* is the desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location (JP 3-58). It states the end state of the MD operation. An MD operation often requires substantial resources that would otherwise be applied directly against the adversary. Consequently, commanders visualize a deception objective in terms of its specific contribution to accomplishing the mission. Any MD operation should create an exploitable advantage at a specific time or place. A deception objective is stated as a positive result, for example—

- Increase friendly force relative combat power at decisive points.
- Provide time for unhindered friendly force entry activities.
- Gain and exploit surprise.
- Protect friendly capabilities and intentions from compromise.
- Achieve a significant advantage in operational timing.

- Enable the force to reach objectives with minimal opposition or resource use.

4-16. If the deception objective is stated in terms of its contribution to the accomplishing the mission, the deception working group (DWG; see paragraph 4-57) refines it into one or more subordinate deception objectives. A ***subordinate deception objective*** **is a restatement of the deception objective in terms that reflect the deception target's point of view.** Subordinate deception objectives state what the deception will lead the target to do or not do. Properly worded subordinate deception objectives can be used as IO information requirements (IRs) or requests for information (RFIs). Figure 4-2 shows examples deception objectives supported by subordinate deception objectives.

Deception Objective (stated in terms of advantages the MD operation will provide the force)	**Subordinate Deception Objectives** (stated in terms of what the MD operation will lead the adversary to do)
This deception will— *Improve my relative combat power in a given location.*	My adversary will— • *Redeploy his reserve to the wrong place.* • *Commit his main forces in the wrong place.* • *Delay the commitment of his reserve.* • *Withdraw his forces*.
This deception will— *Provide a period for defensive preparations.*	My adversary will— • *Conduct additional reconnaissance.* • *Delay his attack to await reinforcements.* • *Prepare for defensive operations.* • *Redeploy his forces to a "threatened" area*.
This deception will— *Provide cover for the withdrawal of my forces.*	My adversary will— • *Not press an attack or pursuit of my forces.* • *Redeploy his* forces *to a "threatened" area.*

Figure 4-2. Relationship of Subordinate Deception Objectives to Deception Objectives

4-17. Subordinate objectives can take several forms. However, all are stated in terms of causing adversaries to do something, for example—

- Delay a decision until it is too late to affect the friendly operation.
- Select or not select a specific course of action (COA).
- Employ or array their forces in ways that make them vulnerable to friendly attack.
- Reveal strength, dispositions, capabilities, and intentions by prematurely committing forces.
- Not react to friendly actions (due to being conditioned to patterns of friendly behavior).
- Waste combat power with inappropriate or delayed actions.
- Withhold an appreciable amount of force to account for uncertainties.
- Shift his effort away from the friendly decisive operation.

4-18. It is not enough for the deception target to believe something about the situation; success requires the target to act on that belief. Commanders—both friendly and adversary—act based on their situational understanding.

They arrive at their situational understanding, in part, by applying judgment to answers to their commander's critical information requirements (CCIR). (See FM 6-0.) An effective MD operation substitutes *desired perceptions* (see definition, paragraph 4-36) for true answers to the target's CCIR. It provides false information about those aspects of the situation upon which the target makes decisions.

CENTRALIZE CONTROL

4-19. Commanders make one individual responsible for overseeing an MD operation. The military deception officer (MDO), the special staff officer responsible for MD, is a member of the IO cell and supports the G-7. (See appendix F.) Based on recommendations from the MDO, the G-3 integrates MD into the operation. This ensures the MD operation does not conflict with other objectives and that all elements portray the same deception story. Execution of the MD operation may be decentralized as long as all participants follow one plan.

EMPLOY VARIETY

4-20. The *deception story* is a scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception (JP 3-58). It is a detailed and systematic expansion of the perceptions and indicators into a complete narrative. Perceptions are mental images the commander wants the deception target to believe are real. An *indicator* in intelligence usage is an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action (JP 1-02).

4-21. MD operations portray indicators that reflect intentions or capabilities that the friendly force commander does not have. The adversary intelligence system may overlook or disregard indicators essential to the deception story if they are transmitted by a single source. The deception target should receive all indicators, both true and false, from multiple sources. This situation lends credibility to the deception story, allows its "verification," and provides the target with more opportunities to conclude that the deception is real. However, if indicators are unusually easy to obtain or if the target suspects the sources, this awareness may arouse enough suspicion to compromise the deception.

4-22. The friendly actions that the deception story outlines are deception events. A *deception event* is a deception means executed at a specific time and location in support of a deception operation (JP 3-58). Indicators are portrayed by deception means.

4-23. *Deception means* are the methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: physical, technical, and administrative (JP 3-58). (The complete joint definition includes definitions of the categories.) While objectives, targets, and available resources are different at each echelon, the basic deception means are the same.

4-24. *Physical means* are activities and resources used to convey or deny selected information to a foreign power (JP 3-58). (To apply this definition to

the operational and tactical levels of war, the Army considers *foreign power* to mean *deception target*.) Physical means present visual indicators through the physical activities of forces. Adversary ground, aerial, and space ISR capabilities offer major avenues for projecting the deception story. Physical means provide indicators that adversary ISR systems report. Physical means include—

- Reconnaissance unit operations.
- Alert and movement of forces.
- Training, testing, evaluation, and rehearsal activities.
- Dummy and decoy equipment, devices, and displays (see FM 20-3).
- Smoke and obscurants (see FM 3-50).
- Logistic, stockpiling, and repair activities.
- Feints, demonstrations, and ruses (see FM 3-90).
- Sonic indicators, which reproduce common noises of military activity. (Such noises are directed against adversary sound ranging sensors and the human ear. Sounds can be real or simulated. The deception plan may also require that the adversary not hear certain sounds; such instances require strict noise discipline.)
- Olfactory indicators, which project battlefield smells to deceive human and technical sensors. (Examples of olfactory deception measures are the creation of odors common to military units and operations, such as those of food, explosives, and petroleum products.)

4-25. *Technical means* are military materiel resources and their associated operating techniques used to convey or deny selected information to the deception target through the deliberate radiation, reradiation, alteration, absorption, or reflection of energy; the emission or suppression of chemical or biological odors; and the emission or suppression of nuclear particles (JP 3-58). (To apply this definition to the operational and tactical levels of war, the Army considers *foreign power* to mean *deception target*.) Electromagnetic deception is an important technical means. Electromagnetic deception includes—

- Manipulative electronic deception—actions to eliminate revealing, or convey misleading, electromagnetic indicators.
- Simulative electronic deception—actions to simulate friendly, notional, or actual capabilities to mislead adversary forces.
- Imitative electronic deception—the introduction of electromagnetic energy into adversary systems that imitates adversary emissions.

4-26. With the advent of advanced multispectral sensors mounted on air and space platforms, electromagnetic deception is growing more complex. However, its basic objective—to manipulate, falsify, or distort the electromagnetic signals received by adversary sensors—is unchanged (Electromagnetic deception is also a method of electronic attack. See chapter 1).

4-27. *Administrative means* are resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to the deception target. (To apply this definition to the operational and tactical levels of war, the Army considers *foreign power* to mean *deception target*.) An example of administrative means is planting bogus material.

4-28. The most effective way to convince the deception target of the deception story's truth is to provide indicators in several different ways, each supported by different elements of truth. Wherever the target turns, there must be information that confirms his preconceptions, that makes any questionable parts of the deception story seem believable. The best way to ensure the story is believable to the target is to present a significant amount of truth in ways that confirm the target's preconceptions.

ENFORCE STRICT OPERATIONS SECURITY

4-29. Successful MD operations require strict operations security (OPSEC). Adversaries must be denied knowledge of the MD operation's existence. Protecting MD operations requires limiting the number of witting actors. (**A *witting actor* is an individual participating in the conduct of a military deception operation who is fully aware of the facts of the deception.**) Only staff and subordinate commanders who need to know are informed of an MD operation. To ensure both secrecy and realism, unwitting actors are often tasked to portray deception events. (**An *unwitting actor* is an individual participating in the conduct of a military deception operation without personal knowledge of the facts of the deception.**) Commanders limit knowledge of the MD operation's details to those who—

- Provide effective feedback.
- Control execution.
- Maintain balance among operational priorities.
- Assess the potential for inadvertent compromise.

MINIMIZE FALSEHOOD/LEVERAGE TRUTH

4-30. Although the deception story uses false information to shape the deception target's perceptions, the less it relies on falsehoods, the smaller the risk of compromise. Even when the deception story's central elements are false, the preponderance of information that creates the target's perceptions is inevitably factual. A deception should use only the amount of false information necessary to produce the desired and supporting perceptions.

4-31. Releasing truthful information to an adversary runs counter to OPSEC. However, it may be necessary to reduce the deception target's uncertainties about conclusions based on the false information that the deception story conveys. Consequently, a delicate balance must be achieved between OPSEC requirements and MD requirements. Obtaining the greatest credibility at the least cost in OPSEC requires skillful planning.

ENSURE TIMELINESS

4-32. The time needed to conduct an MD operation must be less than the time needed for the deception target to react to it. Applying this principle requires two actions: First, determine the time by which the target must act (or fail to act) if the friendly force is to exploit the deception objective. Then reverse-plan all friendly and adversary activities from that time. The G-7 ensures that the time required to conduct the MD operation fits the time available, based on the mission and concept of operations.

ENSURE INTEGRATION

4-33. An MD operation must be fully integrated with the overall operation. MD planning occurs simultaneously with operations planning. Development of the MD plan occurs during the COA development, comparison, and approval tasks of the MDMP.

EXPLOIT TARGET BIASES

4-34. Most people have biases that affect their decisions. Determining the deception target's biases can be the most powerful weapon in the MD planner's arsenal. However, such information is not essential to preparing a viable MD plan. When the target's specific biases are not known, an MD plan can be prepared based on biases of the target's ethnic group or culture. Knowing these biases helps MD planners determine perceptions that will lead the target to act. It also provides clues as to whether and when to increase or reduce the target's uncertainty.

4-35. ***Perceptions*** **are mental images the commander wants the deception target to believe are real**. They include the personal conclusions, official estimates, and assumptions about friendly force intentions, capabilities, and activities that the target uses to make decisions. There are two types of perceptions: desired and supporting.

4-36. A *desired perception* is what the deception target must believe for it to make the decision that will achieve the deception objective (JP 3-58). For example, if the deception objective is for the target to commit additional ground forces to coastal defense at the expense of other areas, the target must believe that an amphibious threat current defending forces cannot handle exists.

4-37. ***Supporting perceptions*** **are mental images that enhance the likelihood that the deception target will form the desired perceptions and accept them as true**. Expanding the example above, if the target is led to conclude that friendly forces consider a land attack too costly, it will likely bolster his confidence in the desired perception that the main threat is from the sea.

4-38. ***Forms of uncertainty*** **are, in military deception, means of shaping the deception target's perceptions. Increasing uncertainty aims to confuse the deception target. Reducing uncertainty aims to reinforce the deception target's predispositions.**

4-39. Decisionmakers can be deceived because they operate in an uncertain environment. Uncertainties about the situation and the inability to predict outcomes accurately require commanders to take risks. Commanders can take advantage of the deception target's uncertainty in one of two ways: they can either increase it or reduce it.

4-40. *Increasing uncertainty* aims to confuse the deception target. This confusion can produce different results: It can cause the target to delay a decision until it is too late to prevent friendly mission success. It can place the target in a dilemma for which there is no acceptable solution. It may even reduce some targets to inaction.

4-41. *Reducing uncertainty* aims to reinforce the deception target's choice of action that best benefits Army forces. It seeks to elicit or prevent a particular adversary COA by supplying the target with enough information to make a firm, but incorrect, decision.

4-42. For an MD operation to be successful, the deception target must believe the deception story, both its parts and as a whole. A good story conforms to the target's beliefs about reality. It is much simpler to have the deception conform to the target's beliefs than to attempt to change them. A target's beliefs include his preconceptions of US doctrine, strategy, objectives, and values. These preconceptions often differ from views Americans hold of themselves.

4-43. As a rule, a deception story should not portray a reality that would surprise the deception target. If parts of the story do not fit into the target's preconceptions, they may create enough suspicion to reveal the deception. People normally accept information that conforms to their preconceptions. Such information must be disproved to become ineffective. Conversely, elements that go against the target's preconceptions will have to be proved true before the target accepts them. Even when all pieces of the story are believable, if enough of them do not fit the target's preconceptions, their overall effect may be inconsistent with the target's existing beliefs. In such cases, the target is likely to ignore the deception story.

4-44. Taking advantage of biases exploits the deception target's own reasoning and preferred choices. Most people are unaware of how deeply their biases influence their perceptions and decisions. The influence of biases is very strong. In many instances, the target may believe a well-crafted deception story until it is too late to act effectively, even in the face of mounting contradictory evidence.

4-45. Nearly any bias can be exploited. When the group that advises the deception target shares a bias, exploiting it is more likely to succeed. However, MD planners must not fall into the trap of believing that the target shares their perceptions, values, or thought patterns (ethnocentricity). All people and cultures are different. Effective MD planners are aware of these differences.

AVOID WINDFALLS

4-46. Clever adversaries suspect indicators that are too easily obtained. Indicators that "fall" into adversary hands must be presented so that the circumstances appear believable, given friendly security practices. There are two ways to achieve this: The first is the *unintentional mistake*, designed to make the target believe that he obtained the indicator due to a friendly error or oversight. The second is *bad luck*, designed to make the target believe that he obtained information because the source fell victim to uncontrollable circumstances.

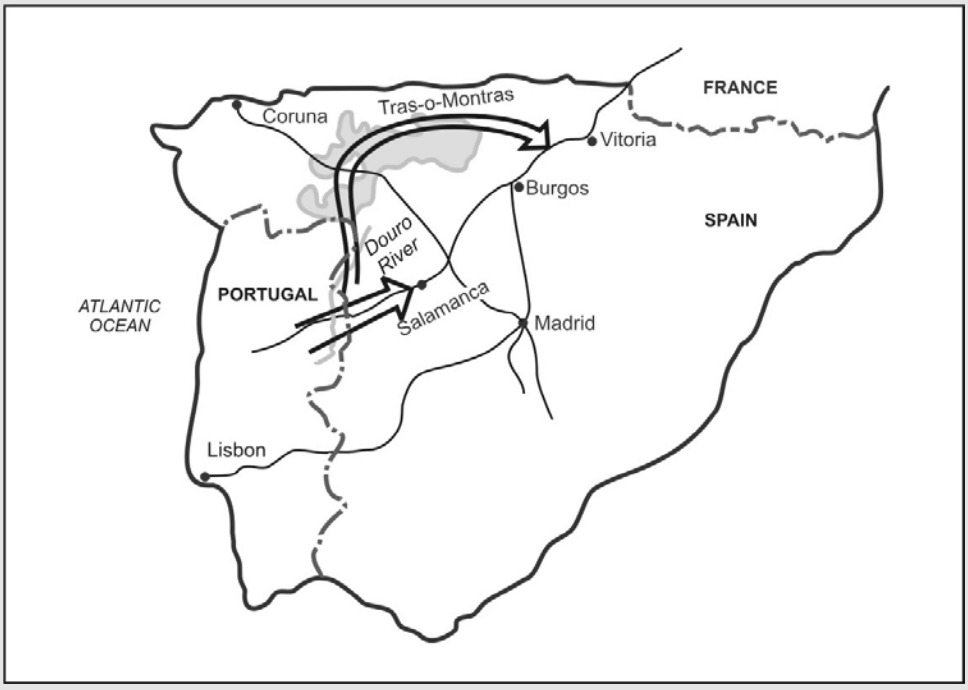
USE SPACE EFFECTIVELY

4-47. For the target to believe the deception story, it must fit the physical and operational environment. A story supporting a tactical deception must be

consistent with how the deception target expects friendly forces to use terrain. Portraying a force in a region unsuitable for military operations or portraying a large force in an impossibly small area is not believable.

Exploiting a Bias: Duke of Wellington in Spain

An MD plan need not be complex to work. A plan executed by the Duke of Wellington, commander of British forces during the 1813 campaign against Napoleon's army in Spain, provides an example of a simple, effective deception. (See Map 4-1.)



Map 4-1. Battle of Vitoria

During his advance toward Vitoria, Wellington decided to envelop the French defenders and force them to yield rather than conducting a frontal attack. Wellington divided his 90,000-man army into two unequal columns. He moved the larger force through a wilderness the French believed impassable while sending a smaller force of 30,000 troops along the expected avenue of approach toward Salamanca.

Knowing the French expected him to lead the main effort, Wellington placed himself in plain view at the head of the smaller force on the expected route. The main Allied advance was made in the north by the left wing of the army under Sir Thomas Graham. It crossed the Douro River and marched through northern Portugal and the Tras-o-Monters Mountains before swinging down behind the French defensive lines. The advance was aimed at Burgos, with a possible follow-on operation of moving to the Pyrenees and into southern France.

Wellington anticipated that the French would conclude that he was leading the decisive operation. Diverting the French commander's attention allowed the enveloping force, the real decisive operation, to move undetected to a flanking position. Having created the deception, Wellington secretly departed to join the larger force as it completed its flanking movement.

Wellington skillfully played on his adversary's preconceptions, which he knew were based on his own tactical habits. He created a ruse that contributed to successfully outflanking the French army while allowing him to be at the decisive point at the decisive time. The Battle of Vitoria ended Napoleon's domination of Spain. This is a classic example of integrating offensive IO into a scheme of maneuver.

WORK WITHIN AVAILABLE COMPETENCIES AND RESOURCES

4-48. The DWG (see paragraph 4-57) always works within the capabilities, experience, and skills of individuals and units available to support the MD. However, MD competencies can be developed through training just as other skills can. MD training in peacetime will increase the chances of MD success during operations.

4-49. MD operations require a diverse array of resources. The resources invested in an MD operation must be adequate to achieve its objective. The concept of operations for the MD operation, deception objective, and higher echelon support determine the resources needed. Commanders weigh the resource costs of an MD operation and ensure that sufficient resources are made available to support it. As all three examples in this chapter show, successful MD operations often require significant resources. However, depending on the concept of operations for the MD operation, these resources may be available for use later in the overall operation. United States Central Command's (CENTCOM's) use of the IV Marine Expeditionary Force and 1st Cavalry Division during Operation Desert Storm illustrate this.

4-50. Corps and higher headquarters control the resources required to conduct operational MD operations. Normally divisions conduct tactical MD operations. However, divisions may execute tactical MD operations as part of a corps operational MD operation.

MILITARY DECEPTION IN THE CONDUCT OF OPERATIONS

4-51. Although attaining complete surprise may not be possible, MD can still be effectively applied in offensive, defensive, and stability operations. MD is rarely appropriate in support operations.

ARMY SUPPORT TO JOINT DECEPTION OPERATIONS

4-52. In joint operations, the ARFOR integrates Army MD operations with joint force MD operations to ensure unity of effort. ARFORs coordinate MD operations with the joint force deception staff element. Normally, ARFORs provide liaison to the deception staff element. When an Army command

functions as a joint task force, the MDO establishes the deception support element to accomplish the same tasks as the DWG (see paragraph 4-57) in corps and divisions.

MILITARY DECEPTION IN THE DEFENSE

4-53. MD operations can allow a defender to offset an attacker's advantage or conceal friendly force vulnerabilities. Typical deception objectives that support the defense are—

- Cause the deception target to delay or misdirect an attack.
- Cause the deception target to not attack at all.
- Confuse the deception target about the defense's depth, organization, or forces.
- Mislead the deception target regarding the duration of and reason for the defense.

Military Deception the Defense: Kursk

In the spring of 1943, the German army in Russia was recovering from a series of desperate battles to stabilize the front after losing the Sixth Army at Stalingrad. For their summer offensive, the German planners were drawn to a large salient that jutted into their lines near Kursk. It offered an opportunity to concentrate their shrinking combat power in a large encirclement in a relatively narrow AO. (See Map 4-2, page 4-14.)

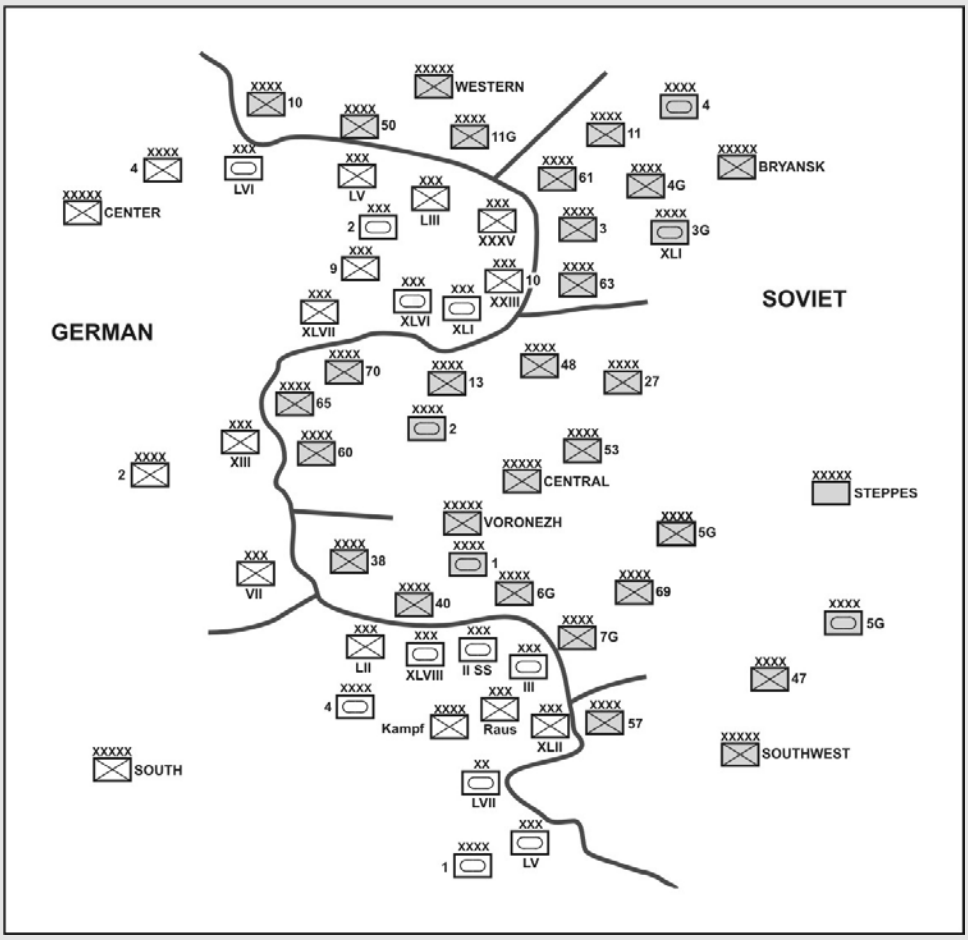
In May, the Russian high command learned of the German plan. Stalin's immediate desire was to launch a series of offensives before the Germans could initiate the Kursk operation. His generals convinced him that a better COA was to defend, absorbing the main blow where they could prepare the battlefield. Once the attacking force had exhausted itself, Russian reserves would launch a series of shattering counterattacks.

The Russians developed a comprehensive MD plan to lead the Germans to continue their offensive preparations, while denying them knowledge that the Soviet Army knew about and was preparing for them. The deception objective was to lure the cream of the panzer corps onto a battlefield specially prepared to kill tanks. The weakened German force would then be vulnerable to a massive counterattack and exploitation.

The Russians did the following to support their deception:

- *Front* (army group) and army staffs developed detailed MD plans that specified the MD operation's objective; the means, forces, and resources allocated to it; and deception event timing.
- Defensive preparations in the Kursk salient were not hidden, but their depth and complexity was.
- Strict OPSEC measures concealed the strategic reserve behind the Kursk salient.
- Imitative electronic deception portrayed a false order of battle. Fake vehicle concentrations, dummy minefields and field fortifications, false airfields, and simulated command posts drew German reconnaissance and fires away from actual activities.
- When the Germans attacked, adjacent *fronts* conducted offensive operations to prevent reinforcement of the German attack.

The Germans attacked on 5 July and quickly bogged down in the extensive defenses. The nature of the defense and the presence of a large operational reserve surprised the Germans. When the defense had exhausted German forces, the strategic reserve counterattacked and drove them back towards the Dnepr River.



Map 4-2. Battle of Kursk

The Russian defense at Kursk, supported by an extensive MD operation, created favorable conditions for a decisive counteroffensive. MD was critical to the operation's success because it ensured that the German attack occurred at a place known to the Russians and in a manner they had prepared to defeat and exploit.

MILITARY DECEPTION IN THE OFFENSE

4-54. In the offense, attackers have the initiative and control the objective, tempo, and place of the fight. Such clarity allows commanders to develop

sharply focused deception objectives. Deception events can conceal the attack's timing, scale, scope, and location, or manipulate them to friendly advantage. They can conceal force composition as well as the tactics and techniques used to execute the attack. Deception events can also mask the concentration of friendly forces, help achieve economy of force, and protect the decisive operation from premature detection.

Military Deception in the Attack: Operation Bertram

Today's MD concepts were developed in the North Africa theater of operations of World War II. As early as 1940, the British Eighth Army had established a staff responsible for integrating MD into operations. The years of experience applying MD paid off with the support provided to British GEN Bernard L. Montgomery's 1942 counteroffensive at El Alamein. (See Map 4-3, page 4-16.)

In the summer of 1942, the British had halted the German Afrika Korps, under Field Marshal Erwin Rommel, at a defensive line extending 35 miles south from the Mediterranean coast at El Alamein. Poor logistic support and lack of replacements forced Field Marshal Rommel to defend. Field Marshal Rommel expected the British to attack but did not know where or when. GEN Montgomery recognized that strategic surprise was impossible, so he planned to gain tactical surprise.

The logical place for the British to attack was at the north of the defensive line. This area contained well-developed logistic sites and the theater's main supply route. Based on their initial intelligence assessment, the Germans placed their armored reserves and strengthened their defenses to meet an attack there.

GEN Montgomery's deception objective was to achieve a favorable correlation of forces in the north, where he intended to conduct his decisive operation. The subordinate deception objectives were to cause the Germans to deploy their armored reserves to the south and delay their response to the attack in the north until D + 4.

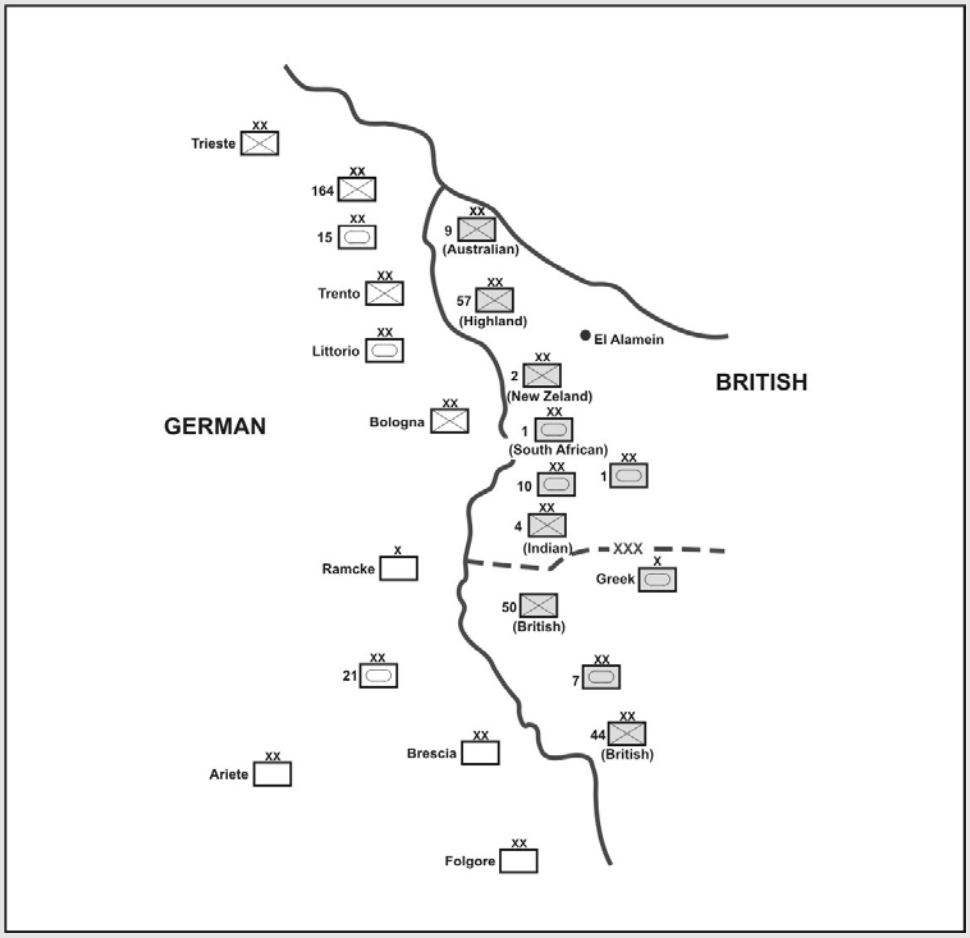
The following are representative deception events used to support the deception objectives:

- Armored formation training exercises emphasized a southern orientation. Dust and smoke reduced visibility, and the Germans were unsure of what was happening.
- Known adversary agents were told the attack would not occur until early November due to mechanical problems with newly arrived, American-made Sherman tanks.
- Artillery positions in the north were disguised as small logistic dumps.
- Dummy artillery sites were constructed in the south.
- Using simulated truck covers, tank concentrations in the north were disguised as logistic marshaling areas.
- Simulated logistic activity in the south portrayed the support needed by a large armored force to conduct offensive operations. Actual support operations occurring in the north were concealed.

The MD operation was a success. Field Marshal Rommel, expecting an attack in early November, returned to Germany and missed the start of the attack on 23 October. The armored reserves were held in the south until D + 4. When committed, they arrived

too late to have a decisive effect. The tactic GEN Montgomery used to initiate the attack—infantry achieving the breach—also confused the Germans.

Operation Bertram demonstrated that the desert's lack of concealment was not an insurmountable obstacle to successful MD operations. Deception objectives were achieved with demonstrations and maneuver. It also showed that, even against a vigilant and skilled opponent, MD could provide significant support to an offensive operation by masking the plan's critical aspects: the when and the where.



Map 4-3. Battle of El Alamein

MILITARY DECEPTION IN STABILITY OPERATIONS

4-55. Depending on the objectives and rules of engagement, MD may be appropriate in a stability operation. When mission transparency is not required, MD can be used to—

- Protect the force by deterring local elements from hostile acts.

- Mask intentions.
- Encourage cooperation among belligerent parties.
- Conceal the timing, circumstances, and conditions of withdrawal upon mission completion.

4-56. The use of deception in stability operations must be carefully weighed against immediate and long-term political impacts. Determining deception objectives will likely require ingenuity. Because many stability operations are also crisis action responses, available time and intelligence may restrict the opportunity to use MD. When MD operations are appropriate, the following conditions apply:

- Political goals and objectives often prevail over military considerations. Deceptions that are perfectly logical from a military perspective may not be appropriate for political reasons. Deceptions that the US considers benign may be considered hostile by the deception target and his supporters.
- Because of political sensitivities, coordination and approval of MD plans can be both lengthy and complex.
- Because conditions are often chaotic, it may be difficult to identify suitable deception targets.
- If the adversary intelligence system is weakly organized or technologically unsophisticated, the number of exploitable information systems (INFOSYS) may be very small. Some technical means may not work.
- Military activities and personnel are usually readily accessible to the general populace during most stability operations. This may offer opportunities to use the local populace as a conduit to the target.

DECEPTION WORKING GROUP

4-57. Because of the size and the diverse range of skills required for an MD operation, the MDO normally forms a DWG. It is tailored to bring together the special technical skills required to conduct a specific MD operation. The MDO relies on the DWG to coordinate the MD operation. The G-7 helps the G-3 integrate the MD operation into the overall operation. As the MD operation proceeds, group membership may change to reflect requirements. When forming the DWG, the MDO balances OPSEC concerns with assurance that the requisite technical skills are adequately reflected during each phase.

SECTION II – CONDUCTING MILITARY DECEPTION OPERATIONS

4-58. Like other operations, MD operations conducted by Army forces follow the operations process (see FM 3-0). (Joint staffs follow the deception planning process established in JP 3-58.) During the operations process, the situation—and consequently many of its associated time factors—are likely to change. The MDO stays abreast of the situation. Planning and preparing in isolation results in a deception that does not correspond to reality and is therefore useless. Planning, preparing, and executing are subject to continuous assessment.

4-59. MD operations start with defining the deception goal, what the commander wants to accomplish with the MD operation. The DWG determines how the adversary (deception target) needs to act in order to accomplish the commander's goal for the MD operation.

4-60. For the MD operation to succeed, the DWG must understand how the deception target acquires and acts on information, what knowledge the deception target has, and how the target views the friendly force. After determining this information, the DWG constructs the deception story. The deception story is a plausible, but false, view of the situation, which will lead the deception target into acting in a manner that will accomplish the commander's goal. Once the story is completed, the DWG determines the deception means necessary to portray the events and indicators, and identifies the units to execute them.

4-61. Part of planning an MD operation is emulating the deception target's decisionmaking process. This includes determining how the target's reconnaissance and surveillance systems observe deception events and collect indicators that support the deception story. It also includes evaluating how the target's intelligence system is likely to process the indicators and whether it will portray them in a form that will allow the target to reconstruct the deception story. Only then can the DWG determine if the reconstructed deception story will cause the target to form the desired perceptions and whether these perceptions will cause the target to act in the desired manner (uncertainties*).* This analysis considers the time the deception target requires to perform these steps and issue the orders that will cause the adversary force to act in a manner consistent with the deception objective.

PLANNING

4-62. Planning develops the information needed to prepare, execute, and assess MD operations. MD planning proceeds concurrently with planning for the overall operation and follows the MDMP. The G-7, assisted by the MDO, participates in planning the overall operation and coordinates the MD operation with the G-3 to ensure it is synchronized with the overall operation. The MDO keeps a log of significant deception planning actions and resources expended. This log becomes the basis of the deception after-action report (AAR).

4-63. Because MD operations support a range of missions, personnel responsible for conducting them remain aware of all higher- and lower-echelon deception activities. To prevent one unit's MD operation from compromising another's, all MD operations are coordinated horizontally and vertically, and approved by the headquarters two echelons higher.

RECEIPT OF MISSION

4-64. Two authorities can direct an MD operation: a higher headquarters and the commander. In both cases, the command's deception plan is coordinated with higher headquarters. When the requirement to prepare the plan for an MD operation is received, the MDO assembles the DWG and begins a mission analysis for a possible MD operation.

4-65. The requirement to support a higher headquarters MD operation can take the form of specified tasks (for example, Position a unit at a certain

location to support the deception story) or IO objectives. The appropriate coordinating staff section oversees execution of specified tasks. The G-7 incorporates IO objectives assigned by higher headquarters into the IO concept of support. This includes developing IO input matrices in the same way as IO objectives that support the command's own operations (see chapter 5).

MISSION ANALYSIS

4-66. The mission analysis for an MD operation proceeds concurrently with the overall mission analysis. The MDO, with the G-7 and G-3 plans, staffs developing MD COAs. A commander who has a firm understanding of the force's deception capabilities may include initial MD planning guidance in the commander's initial guidance, issued during receipt of mission. Otherwise, the commander relies on the staff to provide information on MD capabilities and opportunities. In that case, the staff performs the mission analysis for a possible MD operation and briefs the commander. The commander then issues guidance for MD and the MDO develops MD COAs.

4-67. MD plans require highly specialized and detailed information regarding friendly capabilities and adversary vulnerabilities. An MD operation that cannot be adequately supported with information is not viable. Obtaining this information requires timely and accurate intelligence. The G-7 understands the supporting intelligence system and works closely with the G-2 to obtain responsive intelligence preparation of the battlefield (IPB) and deception-related intelligence support. MD operations take longer to prepare than other types of operations, so early preparation is key to success.

Military Deception Database

4-68. Before starting to plan, the MDO prepares a database to support potential MD COAs. This database contains information needed to determine ways an MD operation can support the overall operation. It includes information about the current situation and foreseeable conditions that are not specific to a particular mission. The commander needs this general information to objectively determine how an MD operation could support a specific mission. Accurate knowledge of force capabilities prevents underusing deception assets or attempting to use nonexistent capabilities. Both errors divert resources better used elsewhere. The MDO and DWG build and continually update the MD database. External intelligence elements may be asked to support them.

4-69. Being aware of one's ability or inability to influence a potential deception target is the first step in avoiding risks and conducting successful MD operations. The MD database requires two types of information on any potential adversary:

- Information about adversary doctrine and capabilities.
- Information about the adversary's intelligence system and decisionmaking process.

4-70. The first category concerns the adversary's forces and concept of military art. In a stability operation, it may include information about the adversary's ideology, view of the struggle's context, and appropriate means. It

includes data on the adversary's C2 and intelligence systems. Most of this information is collected as part of normal IPB.

4-71. The second category concerns adversary procedures for collecting and analyzing data. It includes how the deception target makes decisions and any matters that can influence these decisions. This part of the MD database should include the characteristics and personalities of potential deception targets, including the characteristics that define their degree of susceptibility to deception. The second category provides tools needed to best use the first category. This information is necessary for the MD planner to emulate the target's thought process. Developing the levels of awareness needed to conduct emulative role-playing of the more important potential targets is an MD goal. Key DWG members should be able to play the role of the adversary commander during COA analysis.

4-72. The MD database contains specific information on friendly MD means. It includes information on friendly doctrine and tactics, technical characteristics of combat systems, and friendly intelligence and counterintelligence resources and operations.

Military Deception Estimate

4-73. The output of the MD mission analysis is the MD estimate, prepared by the MDO. (FM 5-0 discusses staff estimates. Appendix C discusses the IO estimate.) It provides information, capabilities, MD opportunities, and recommendations on feasible deception objectives. The MDO presents this estimate during the mission analysis briefing. The estimate considers the limitations of current capabilities based on deception target susceptibilities, available time, and available MD means. The commander considers the MD estimate in developing the commander's guidance.

Military Deception Guidance

4-74. The commander issues MD guidance as part of the commander's guidance at the conclusion of mission analysis. It establishes the role that MD is to play and is usually expressed as one or more deception objectives. In that case, no further planning guidance may be needed. Alternatively, the commander may describe the possible role for MD, leaving the staff to recommend specific deception objectives. If the staff is asked to make recommendations for deception objectives or if the commander provides no guidance for MD, the MDO proposes deception objectives. If there are no MD opportunities or the commander decides that the risks do not justify the costs, then MD is limited to MD in support of OPSEC. MD in support of OPSEC aims to prevent compromise of sensitive or classified activities, capabilities, or intentions. It seeks to deny adversaries a clear picture of what is occurring within the AO by targeting adversary intelligence functions.

COURSE OF ACTION DEVELOPMENT

4-75. After receiving the commander's guidance for MD, the DWG develops MD COAs while the G-3 develops COAs for the overall operation. The G-3-developed operational COAs provide the basis for MD COAs. Basing MD

COAs on operational COAs ensures MD COAs are feasible and practical. Preparing an MD COA includes six tasks—

- Develop the deception story.
- Identify the deception means.
- Determine the feedback required for assessment.
- Conduct a risk assessment.
- Conduct an OPSEC analysis (see chapter 3).
- Plan for termination.

Develop Deception Story

4-76. Deception story development is an art and a science. It combines intelligence on adversary information collection, processing, and dissemination; how adversary preconceptions are likely to influence the deception target's conclusions; and how the target makes decisions. The story is built and stated exactly as the DWG wants the target to reconstruct it.

4-77. The DWG derives the candidate deception story from indicators that will lead the deception target to the desired perceptions. It weaves deception events together into a coherent whole that describes the situation that the commander wants the target to perceive. The story is always written from the target's perspective, what the target is expected to see and think as he sees indicators and assimilates them into his commander's visualization.

4-78. If the deception target is to develop the desired perceptions, the deception story must be believable, verifiable, and consistent. The story must be doctrinally correct and consistent with the situation. For example, if a unit that has traditionally followed sound practices of signature reduction blatantly violates that discipline, the deception target would probably suspect a deception event. Ideally, the MD planner wants the deception story to be the exact mental picture the target forms as the MD operation unfolds. Simply stated, the deception story should read like the deception target's own intelligence estimate.

4-79. Each deception story element is associated with a deception means that can credibly portray the required indicators. The MD COA identifies how the adversary C2 system should transmit this information to the deception target. The DWG anticipates that various nodes in the C2 system will filter the information conveyed, introducing their own predispositions and biases.

4-80. The finished deception story is like a completed jigsaw puzzle. It allows the DWG to check the logic and consistency of the MD COA's internal elements. The group can then identify perceptions, indicators, and deception events that need refinement. The check also identifies where indicators can be added to strengthen deception events or diminish the effect of competing indicators.

Identify Deception Means

4-81. During this task, the DWG further refines the desired perceptions. The nature of these perceptions, the number of them required, and the supporting indicators needed to convey them to the deception target in a believable fashion determine the MD operation's complexity.

4-82. As the DWG integrates indicators into deception events, it ensures that they are consistent with the friendly force operational profile and that adversary ISR systems are likely to detect them. The group determines which adversary ISR elements to target. For example, indicators may be collected by an adversary communications interceptor, reported to an intelligence analysis center, included in a command intelligence summary, and presented to the deception target during a morning intelligence briefing. In this case, the adversary ISR elements include the—

- Intercept operator and equipment.
- Communications intelligence report and means by which it was transmitted.
- Analysis center personnel who handled the information.
- Intelligence summary and the means by which it was transmitted.
- Briefer and the briefing to the deception target.

4-83. An important part of MD planning is determining the adversary ISR assets most likely to observe the deception event and pass it to the deception target. When selecting the assets, MD planners consider—

- How information enters the intelligence system (the collection mechanism).
- What kind of information the intelligence system conveys.
- When ISR assets are available to transmit information.
- How long the information will take to reach the deception target.
- What degree of control the deceiver can exercise over various ISR assets.
- How credible the target believes information from these different sources to be.
- What filters are likely to affect the information as it moves through the intelligence system.

4-84. A principal method of projecting a deception story is to create the illusion of unintentional security breaches. A deception target is likely to believe information derived from apparently isolated and random security violations. The systematic yet seemingly random transmissions of deception story elements by multiple means also makes the deception more believable.

Determine Feedback Required for Assessment

4-85. As, the DWG develops an MD COA, it determines the feedback needed to assess the MD operation. This task includes—

- Envisioning how the deception target would act without the deception.
- Envisioning how the target would respond to indicators and desired perceptions.
- Determining detectable actions that would indicate the target believes the deception story.
- Submitting IO IRs or RFIs to obtain reports of those actions.

Commanders assess MD operations based on feedback. They monitor feedback and compare it against the criteria of success established for the MD operation.

4-86. ***Feedback* is information that reveals how the deception target is responding to the deception story and if the military deception plan is working**. There are two forms of feedback: indicator and perception.

4-87. ***Indicator feedback* is information that indicates whether and how the deception story is reaching the deception target**. It is useful in timing and sequencing deception events. It can also alert the MD planner to the need for additional deception events to effectively portray indicators that have not yet been "seen." Indicator feedback was formerly called "operational feedback."

4-88. ***Perception feedback* is information that indicates whether the deception target is responding to the deception story**. It shows whether the target is forming the desired perceptions and is acting (or likely to act) in accordance with the deception objective. Analytical feedback may be obtained from a variety of target activities, such as questions the target asks the intelligence staff or orders the target gives. Perception feedback was formerly called "analytical feedback."

Conduct Risk Assessment

4-89. All MD operations involve risks and costs. Commanders base the decision to conduct an MD operation on a deliberate assessment that weighs costs against benefits. The MDO performs a risk analysis of each MD COA during COA development using the techniques discussed in chapter 5. They consider the results of this analysis during COA comparison. The MDO presents the risks, benefits, and costs of the recommended MD COA to the commander during COA approval. The commander decides if the potential gains outweigh the risks. Risks are considered during MD planning and continuously assessed and recalculated throughout preparation and execution.

4-90. Any MD operation risks losses if it fails. The possibility of failure stems from the uncertainties involved in how indicators intended for the deception target are received and interpreted as well as how they eventually affect the target's situational understanding. If the MD operation must succeed for the overall COA to succeed, then the MD operation is an essential task. This use of MD usually provides the highest payoff but at greater risk. The G-3 and G-7 ensure that the commander is willing to accept this level of risk before including it in any COA. Deception risks take the following forms:

- **Risk of failure**. If the target sees the deception and all the information, but does not act in accordance with the deception story and objectives the deception fails.
- **Risk of exposure**. If the MD operation is compromised, it may cause the deception target to deduce the actual plan. If discovered, the resources used for the MD operation may be placed in jeopardy. Worst case, a compromised friendly MD operation may be turned against its originator.
- **Risk of unintended effects**. The target may react to the MD operation in an unanticipated way, or unintended third parties may be inadvertently deceived and react to the deception in unforeseen ways. Such

effects can be positive or negative, and may involve either the MD operation itself or other operations.

4-91. The command can mitigate the risks associated with MD operations by applying the following measures:

- Use MD as a shaping operation to enhance mission success, but not as an essential task.
- Identify realistic deception objectives.
- Establish robust intelligence support for the MD operation.
- Anticipate conditions that could compromise the MD operation and plan responses.
- Use emulative red-teaming of the MD operation during planning.
- Continuously assess the command's OPSEC posture.
- Conduct continuous assessment to determine if the adversary believes the deception.

Conduct an OPSEC Analysis

4-92. MD operations create a complex OPSEC challenge. They require commanders to rigorously employ and artfully manipulate OPSEC measures. For an MD operation to succeed, commanders carefully manage OPSEC requirements to provide adequate, but not excessive, protection. Excessive concern about OPSEC can unnecessarily impede the MD operation. The G-7 integrates OPSEC measures into all MD operation phases.

4-93. Deception events frequently portray seemingly careless breaches of friendly OPSEC. These must be accomplished without compromising actual OPSEC practices and other friendly operations. False indicators are usually wrapped in significant amounts of factual information to enhance their acceptance. The G-7 ensures that release of accurate information does not compromise friendly plans or forces. Essential security is maintained, even as the MD operation conveys a controlled flow of factual data.

4-94. Throughout every phase, the MD operation must be protected from both hostile and unintended friendly detection. This requires applying the OPSEC process to MD planning (see chapter 3). First, the DWG identifies, by MD COA phase, the information that would allow the adversary to detect the MD operation. These become essential elements of friendly information (EEFI) related to the MD operation (OPSEC action 1).

4-95. Next, the DWG analyzes the adversary's ability to detect the MD operation (OPSEC action 2). Adversaries can acquire EEFI through either direct detection or systematic analysis. The DWG anticipates that adversary analysis will include not only obvious EEFI, but also second- and third-level indicators that together can reveal an MD operation. To determine OPSEC indicators, the DWG determines how the EEFI are passed internally and where they may "leak out." This analysis of vulnerabilities (OPSEC action 3) is done from the adversary's point of view. It is the crucial task of the OPSEC process. It identifies OPSEC measures that may be used to protect EEFI related to the MD operation. Field support teams from the 1st Information Operations Command (Land) (1st IOC [L]) can assist in this effort (see appendix F).

4-96. When the analysis of vulnerabilities is done, the DWG assesses the risks involved in using or not using individual OPSEC measures (OPSEC action 4). The group considers the results of this assessment during COA comparison. The OPSEC measures for the recommended MD COA are presented to the commander during COA approval. The commander decides which OPSEC measures to implement.

4-97. The commander's approval of an MD COA constitutes direction to implement the OPSEC measures associated with that COA (OPSEC action 5). The OPSEC officer converts approved OPSEC measures into IO tasks and incorporates them into IO planning. IO tasks that implement OPSEC measures are assigned to units in paragraph 3b of the OPSEC appendix to the IO annex of the operation plan (OPLAN)/operation order (OPORD).

4-98. Developing viable COAs is critical to planning an MD operation. Overly ambitious MD COAs risk failure, while overly conservative COAs may leave potential capabilities untapped. The ability to establish viable COAs depends on the DWG's creativity and the extent to which deception capabilities have been developed beforehand.

Plan for Termination

4-99. A MD COA includes the conditions that will result in terminating the MD operation and branches that address them. Termination planning establishes measures to advantageously end the MD operation while protecting deception means and techniques. Termination preparations continue throughout the MD operation. Three actions take place regardless of whether the MD operation reaches its objective or remains concealed. They are—

- The organized cessation of deception activities.
- The protected withdrawal of deception means.
- After-action assessments and reports.

4-100. The MD COA states the risks to sources and means that would outweigh the MD operation's benefits and result in its termination being recommended. It includes termination branches that address each of these circumstances:

- Success.
- Failure.
- Compromise.
- Deception no longer needed.

COA ANALYSIS, COMPARISON, AND APPROVAL

4-101. The staff analyzes MD COAs as it war-games COAs for the overall operation. The MDO establishes criteria for evaluating MD COAs before the war game begins. These criteria usually include the risks and costs of each COA, including those associated with OPSEC measures.

4-102. G-3 planners consider MD COAs when they compare COAs for the overall operation. They analyze the strengths and weaknesses of each MD COA. The ability of an MD COA to support a particular overall COA is one of the factors considered when determining which MD COA to recommend. The G-7 may recommend one to the commander as part of the decision briefing

during COA approval, or in a separate briefing, if OPSEC or other factors make it appropriate. When the commander approves an MD COA, it becomes the concept of operations for the MD operation.

ORDERS PRODUCTION

4-103. The DWG prepares the MD plan after the commander approves an MD COA. (The MD appendix to the IO annex contains the MD plan. Its distribution is usually limited to those with a need to know.) Once the MD plan is completed, coordinated, and reviewed for consistency, it is presented to the commander for tentative approval. To ensure synchronization of MD at all levels, approval authority for MD operations resides two echelons above the originating command. After the approving authority has approved the MD plan, it becomes a part of the OPLAN/OPORD. Approved MD plans that are not intended for immediate execution are updated on the same basis as the supported OPLAN and reviewed through the final approval authority before execution.

PREPARATION

4-104. During preparation, commanders take every opportunity to refine the MD plan based on updated intelligence. While many sources provide updated intelligence, reconnaissance is often the most important part of this activity. Reconnaissance operations are carefully planned so as not to compromise the MD operation. Commanders balance the need for information with the possible compromise of the MD plan by reconnaissance units. Reconnaissance units are normally unwitting participants in MD operations.

4-105. OPSEC activities continue during preparation for the MD operation. As with reconnaissance, OPSEC is a dynamic effort that anticipates and reacts to adversary collection efforts. Unit movements are closely integrated with MD operations and OPSEC measures to ensure they do not reveal friendly intentions.

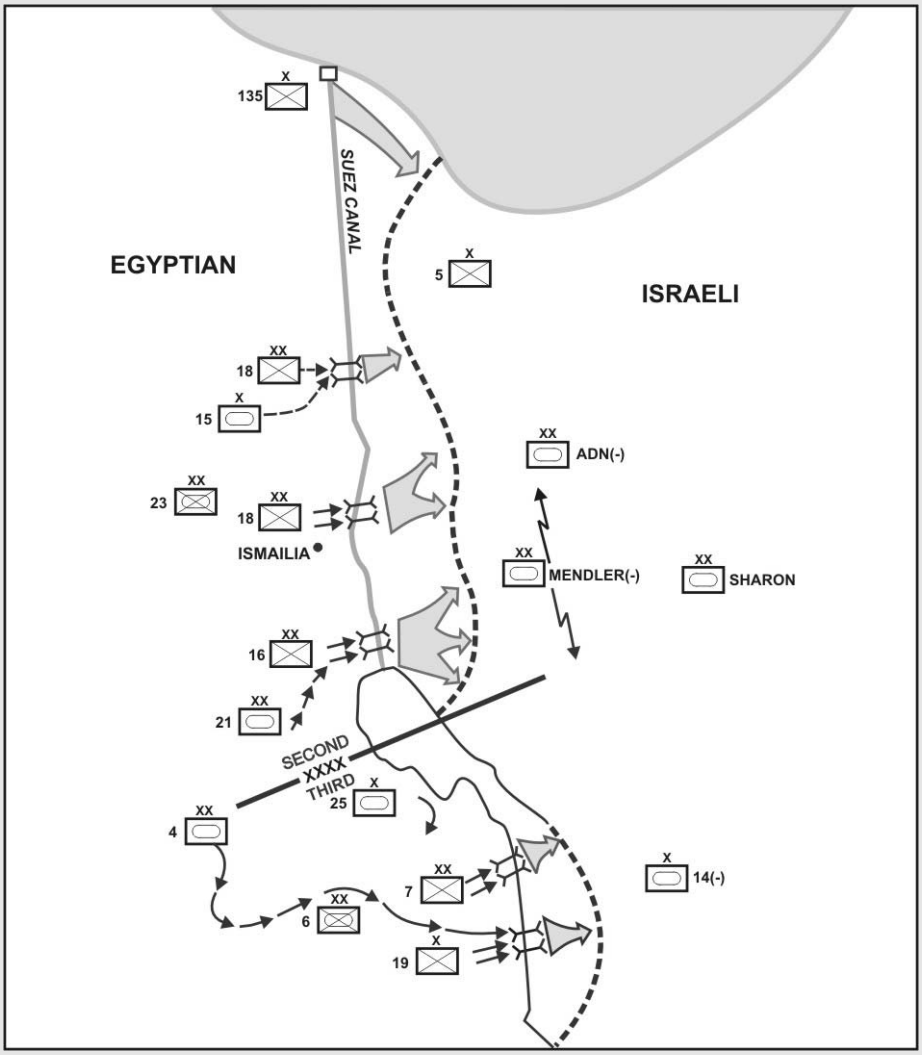
4-106. MD plans are not static. They may be adjusted based on new information. As assumptions prove true or false, adversary perceptions are confirmed, or the status of friendly units change. Commanders adjust the MD operation, or abort it if it can no longer affect the situation significantly.

4-107. Task organization changes are normally done during preparation. Changes connected to an MD operation may be covert. Extensive OPSEC measures are required. The deception plan may be compromised if the adversary detects the changes and perceives no logical reason for them. Conversely, if task organization changes are part of a deception event, subtle OPSEC violations can be used as indicators.

4-108. One preparation technique is to condition potential targets to “set them up” for subsequent MD operations. Conditioning is the process of deliberately creating or reinforcing biases or predispositions that make the target more likely to form desired perceptions. For example, conducting recurring offensive exercises in a given area may cause the target to disregard indications of actual later offensive preparations and believe a deception story designed to cover an intended attack.

Conditioning an Adversary: The Egyptian Crossing of the Suez

The rapid crossing of the Suez Canal by the Egyptian Army at the start of the1973 Yom Kippur War was facilitated by a carefully orchestrated MD operation. The canal-crossing operation was conducted against a highly skilled opponent. The Israeli intelligence service was efficient and could observe the Egyptian rear area with all intelligence disciplines. (See map 4-4.)



Map 4-4. The Egyptian Crossing of the Suez

The Egyptian deception objective was to achieve operational surprise in the initial phase of the attack. The Egyptians sought to do this by denying information on the assault preparations to the Israelis, their own troops, foreign intelligence services, and the media. Egyptian EEFI included details on the timing, scope, and tactical execution of the assault. The subordinate deception objectives were to—

- Cause the Israelis to delay early mobilization.
- Deny the Israelis an opportunity to conduct a preemptive strike.
- Delay the Israeli decision to execute an armored counterattack for at least eight hours after the crossing began.

This was a formidable task. The Suez Canal averages 200 meters wide. From defensive position on the eastern bank, the Israelis could observe any Egyptian preparations.

The Egyptians used deceptive measures and a broad range of centrally directed and controlled deception events involving political and military activities. These included—

- Maintaining a pattern of national-level normalcy in international affairs by not canceling scheduled diplomatic activities and visits by foreign dignitaries.
- Demobilizing 20,000 reservists 48 hours before the attack.
- Providing cover for large numbers of assault troops on the canal by establishing a pattern of maneuvers and training during the six months before the attack.
- Moving assault bridging to the canal by sections at night, placing it in specially dug pits, and covering it with canvas and sand.
- Closing descents to the canal in some areas and opening new ones at others locations.
- Improving defensive position on the Egyptian side of the canal.
- Publishing reports in the press that officers would be allowed leave for the annual hajj pilgrimage.
- Hiding recently purchased, commercial, high-capacity fire-fighting water pumps to conceal their ability to quickly remove large sections of the Israeli sand berm.
- The Egyptian MD operation could not conceal the coming attack, but it did perform a vital function: it concealed how the Egyptians planned to use new technology and the scale, scope, and precise timing of the operation. The Egyptian example illustrates that although it may not be possible to totally conceal one's intent to attack, it may be possible to protect a sufficient number of details associated with the plan by deception. Masking key elements of the plan can give the friendly commander a demonstrable advantage on the battlefield.

EXECUTION

4-109. Execution takes place in a dynamic environment. Consequently, the commander continually assesses and refines the MD operation. As with planning and preparation, assessment is continuous during execution. By its nature, there is little flexibility in an MD operation. The key to success is knowing precisely when to take the next step in conveying the deception

story. The MD plan identifies feedback events and indicators for intelligence collection and analysis to provide these cues.

4-110. An MD operation is executed as part of the overall operation. Executing an MD operation involves controlling and terminating.

CONTROLLING DECEPTION OPERATIONS

4-111. Within command and control, *control* is the regulation of forces and battlefield operating systems to accomplish the mission in accordance with the commander's intent. It includes collecting, processing, displaying, storing, and disseminating relevant information for creating the common operational picture, and using information, primarily by the staff, during the operations process (FM 6-0). In MD, it consists of decisions undertaken while executing the MD operation. It involves deciding to execute each deception event as specified by the MD plan or to change the plan to align it to situational changes or adversary responses. Many deception activities are projected during planning as a part of the progression of events envisioned in the execution schedule. Other decisions are dictated by events revealed during execution. Centralized control over deception events is imperative to ensure they are synchronized in a way that does not conflict with other operations. This requires close coordination among the assets tasked to conduct them. The MD plan's C2 paragraph states the person with authority to order changes to the deception plan.

TERMINATING DECEPTION OPERATIONS

4-112. Terminating the MD operation is the final execution control action. When the termination decision is made, the appropriate termination branch or sequel becomes the basis for a deliberate series of termination events.

4-113. An AAR is an integral part of terminating an MD operation. AARs should include lessons learned as well as deception cost parameters, such as monetary expenditures, materiel and resources, units employed, man-hours needed, and opportunity costs. Cost data provides the G-7, the MDO, and the commander with a concrete basis for evaluating COAs for future MD operations.

ASSESSMENT

4-114. *Assessment* is the continuous monitoring—throughout planning, preparation, and execution—of the current situation and progress of an operation, and the evaluation of it against criteria of success to make decisions and adjustments (FM 3-0). It involves receiving and processing information about implementing the MD operation. It also includes continual reexamination of deception objectives, targets, stories, and means. Control activities include the interim decisions and instructions needed to adjust the MD plan's implementation. Both activities continue until termination activities are complete. There are four types of assessment activities during MD operations:

- Monitoring and evaluating the MD operation to ensure it continues to correspond to actual conditions.

- Obtaining the feedback necessary to evaluate the progress of the deception story.
- Monitoring unintended consequences of the MD operation. Data on unintentional effects may be used to adjust deception events or take advantage of new opportunities.
- Evaluating the need to terminate the MD operation for reasons other than success.

4-115. Experience is a major source of MD planning information. Institutional experience includes AARs and analyses from recent MD operations. These address both potential deception targets and the mechanics of conducting an MD operation. As with other operations, these data are generated during execution. Their collection, processing, and storage end the MD operation. Lessons from all operations process activities—planning, preparation, execution, and assessment—are captured.

4-116. Commanders assess MD operations continually. An MD plan's quality is related to the validity of assumptions concerning what the situation will be when the overall operation starts. Validating such assumptions with updated information is essential to any assessment. To do this, the general situation is continually assessed prior to the overall operation's start. Such assessment may be necessary to determine when to start the MD operation.

PART TWO

Tactics, Techniques, and Procedures

Like all military operations, information operations follow the operations process: planning, preparation, execution, and continuous assessment. These activities are sequential but not discrete; they overlap and recur as circumstances demand (see FM 3-0; FM 6-0). Part Two is organized around these activities: Chapter 5 addresses planning. Chapter 6 addresses preparation. Chapter 7 addresses execution. Since commanders assess operations continuously, each chapter addresses aspects of assessment that apply to the activity being discussed.

Chapter 5

Planning Information Operations

Chapter 5 explains how to use the military decisionmaking process (MDMP) to plan information operations. (FM 5-0 discusses the MDMP.) Each section addresses an MDMP task or a group of related tasks. Appendix A lists the MDMP tasks and the G-7 actions and products associated with them. Appendix B contains a scenario that illustrates the products developed during each MDMP task. This chapter includes cross-references to the examples in Appendix B.

SECTION I – INFORMATION OPERATIONS PLANNING CONCEPTS

5-1. *Planning* is the means by which the commander envisions a desired outcome, lays out effective ways of achieving it, and communicates to his

CONTENTS

subordinates his vision, intent, and decisions, focusing on the results he expects to achieve (FM 3-0). Commanders and staffs above company level use the military decisionmaking process (MDMP) to plan operations. The G-7 follows MDMP techniques to plan and synchronize information operations (IO). The commander's personal interest and involvement is essential to ensure that IO effectively supports accomplishing the mission. To achieve this, commanders and staff planners consider IO throughout the MDMP. Planning IO requires integrating it with several other processes: among them, intelligence preparation of the battlefield (IPB) (see FM 34-130) and targeting (see appendix E and FM 6-20-10). G-2 and fire support representatives participate in IO cell meetings and work with IO cell members to synchronize IO with their activities and the overall operation. Commanders use the IO mission statement, IO concept of support, IO objectives, and IO tasks to describe and direct IO (see figure 5-1).

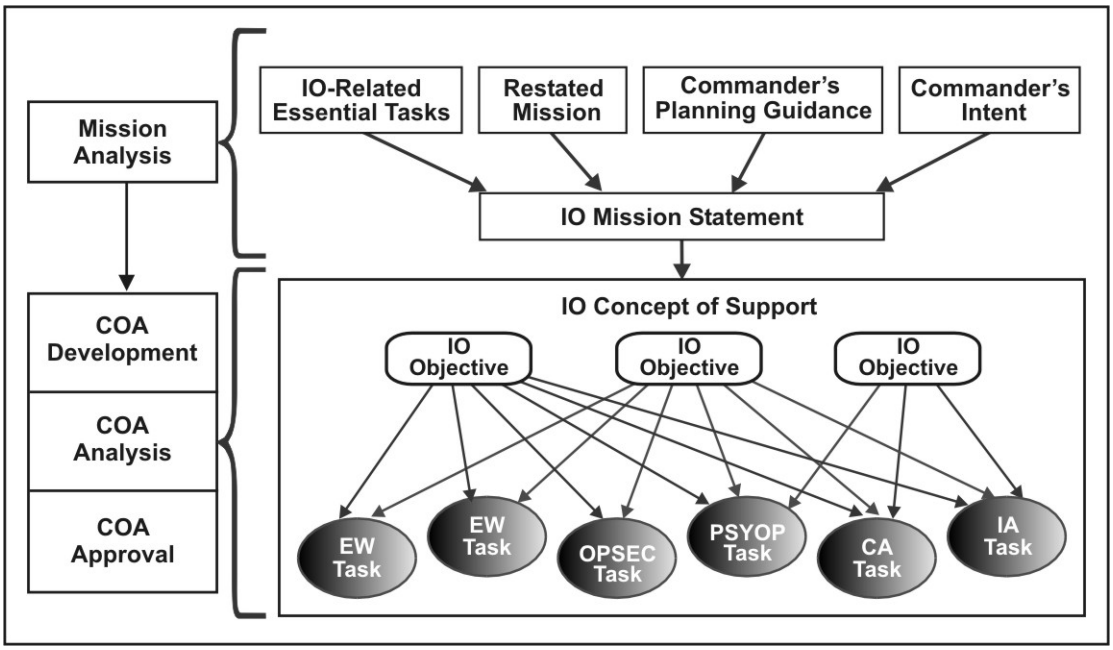


Figure 5-1. Relationship of the IO Concept of Support, IO Objectives, and IO Tasks

5-2. **The *information operations mission statement* is a short paragraph or sentence describing what the commander wants IO to accomplish and the purpose for accomplishing it.** The G-7 develops the initial IO mission statement at the end of mission analysis, based on the restated mission, IO-related essential tasks, commander's intent, and commander's planning guidance. The G-7 develops the final IO mission statement after the commander approves a course of action (COA). The final IO mission statement includes the IO objectives for the approved COA. The IO initial mission statement may include initial IO objectives, if any emerge during mission analysis.

5-3. **The *information operations concept of support* is a clear, concise statement of where, when, and how the commander intends to focus**

the information element of combat power to accomplish the mission. During COA development, the G-7 develops a separate IO concept of support for each COA the staff develops. IO concepts of support are written in terms of IO objectives and IO elements/related activities.

5-4. ***Information operations objectives*** **are clearly defined, obtainable aims that the commander intends to achieve using IO elements/related activities.** IO objectives serve a function similar to that of terrain or force-oriented objectives in maneuver operations. They focus IO on things that must be done to accomplish the IO mission and support the commanders' intent and concept of the operation. IO objectives usually involve tasks by more than one IO element.

5-5. Accurate situational understanding is key to establishing IO objectives. Operational- and tactical-level objectives are more immediate than strategic-level objectives. However, they may also contribute to national- and theater-strategic IO objectives. Joint and component staffs at the operational level integrate and synchronize IO into campaigns and major operations (see FM 3-0).

5-6. The G-7 develops most IO objectives concurrently with IO concepts of support during COA development. At the same time the G-3 develops terrain or force-oriented objectives. However, some IO objectives may emerge during mission analysis. These include IO objectives that are present during all operations: such as, prevent compromise of the operation, and protect C2. Others may be related to specified tasks from the higher headquarters. IO objectives become part of the final IO mission statement. The G-7 uses them to focus the conduct of IO tasks.

5-7. IO objectives for offensive and defensive IO are stated in terms of effects. For offensive IO, these are destroy, disrupt, degrade, deny, deceive, exploit, and influence. For defensive IO, these are protect, detect, restore, and respond (see chapter 1).

5-8. ***Information operations tasks*** **are tasks developed to support accomplishment of one or more information operations objectives.** An IO task addresses only one IO element/related activity. The G-7 develops IO tasks during COA development and finalizes them during COA analysis. During COA development and COA analysis, IO tasks are discussed in terms of IO elements/related activities. During orders production, IO tasks are assigned to units. FM 3-13 uses *IO task* in only one context: to refer to a task that is performed by one IO element/related activity and supports one or more IO objectives. All other tasks that concern IO are referred to as *IO-related tasks*.

5-9. The goal of IO planning is to integrate IO into the overall operation. The G-7 achieves this by developing IO planning products that—

- Express how IO contribute to accomplishing the mission.
- Assign IO tasks to units responsible for performing them.
- Synchronize IO task performance.
- Describe how the command will assess IO.

The most important IO planning product is the IO subparagraph or IO annex of the operation plan (OPLAN) or operation order (OPORD) (see appendix D).

The IO annex usually includes an IO execution matrix and IO assessment matrix as appendixes.

5-10. Integrated IO planning requires innovation and flexibility. Some IO elements/related activities—such as, psychological operations (PSYOP), operations security (OPSEC), and military deception (MD)—require a long lead time for planning and preparation. Some elements must be executed before other aspects of the overall operation. Others demand higher resolution and more up-to-date intelligence. For some, there is a long lag between execution and assessment of their effects. IO require a concentrated intelligence, surveillance, and reconnaissance (ISR) effort during preparation and execution to obtain and analyze information for assessing IO effectiveness. The increased resolution of intelligence, new intelligence data requirements, and the long lead time required necessitate early collection and analysis. These factors increase the challenges facing IO planners and decrease the time available to prepare IO. Nevertheless, early execution of selected IO tasks can enhance efforts to shape the area of operations (AO) and information environment.

5-11. Integral to IO planning is the development and continuous updating of the IO estimate (see appendix C). Some IO elements/related activities, such as PSYOP, maintain separate estimates. All estimates are running (continuously updated) estimates. Maintaining a current IO estimate pays off during orders production because major portions of it contain information that forms the basis for the IO annex and associated appendixes. In addition to supporting the development of the base order and warning orders (WARNOs) during planning, the G-7 uses the IO estimate to plan branches and sequels during preparation (see FM 3-0), and to prepare IO input to fragmentary orders (FRAGOs) during execution.

SECTION II – RECEIPT OF MISSION

5-12. Upon receipt of a mission, either from higher headquarters or from the commander (see figure B-2, page B-3), the commander and staff perform an initial assessment. Based on this assessment, the commander issues initial guidance (see figure B-3, page B-5) and the staff prepares and issues a WARNO (see figure B-4, page B-6). During the time between receiving the commander's initial guidance and issuing the WARNO, the staff performs receipt of mission actions. During receipt of mission, the G-7—

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

5-13. The primary G-7 products are input to the following products and processes: IPB, the initial ISR tasking, and the initial WARNO. The G-7 also determines how much time to allocate to each action and ensures the commander includes IO factors in the commander's initial guidance and WARNO.

PARTICIPATE IN COMMANDER'S INITIAL ASSESSMENT

5-14. The commander's initial guidance emerges from the initial commander's visualization. This process includes an exchange of information between the commander and staff members—typically the G-2, G-3, G-6, G-7, and the fire support coordinator (see FM 6-0). More staff elements become involved later. At this point the G-7 helps the commander visualize the operation by describing how IO can support it. The G-7 bases the advice on the IO estimate.

RECEIVE COMMANDER'S INITIAL GUIDANCE

5-15. Commanders include IO guidance in their initial guidance. Separate guidance on IO may be appropriate during peace operations or other missions where information is the principal element of combat power. However, commanders do not consider IO in a vacuum. When they issue IO guidance separately, they ensure it is consistent with their other guidance. To ensure development of a clear IO concept of support and specific IO objectives, IO tasks, and criteria of success, commanders provide as much specific guidance on IO as possible.

5-16. The commander's initial guidance may include essential elements of friendly information (EEFI) and instructions regarding military deception (MD). Establishing EEFI starts the OPSEC process (see chapter 3). The G-7 reviews existing EEFI and recommends changes, if necessary. If the commander issues MD guidance, the military deception officer (MDO) assembles the deception working group and begins MD planning (see chapter 4).

PERFORM INITIAL INFORMATION OPERATIONS ASSESSMENT

5-17. Once the commander issues initial guidance, the G-7 assembles the IO cell (time permitting) and performs an initial IO assessment. This assessment begins with the IO estimate. The G-7 updates it based on input from IO cell members and identifies any information gaps. In a time-constrained environment, the only information reasonably available may be that in the IO estimate. During this assessment, the G-7 derives guidance from two sources: the commander's initial guidance and the higher headquarters OPLAN/OPORD. These two sources define the IO role in the operation and provide the information needed to start planning. The initial IO assessment results in the following products:

- IO input to IPB.
- IO input to the initial ISR tasking.
- IO input to the initial WARNO.

PROVIDE INITIAL INPUT TO INTELLIGENCE PREPARATION OF THE BATTLEFIELD

5-18. IPB supports IO by identifying the IO capabilities and vulnerabilities of friendly, adversary, and other key groups. It portrays adversary and other key group leaders/decisionmakers, command and control (C2) systems, and decisionmaking processes. IO input to the initial IPB performed during receipt of mission focuses on identifying IO IRs that include information about—

- Adversary and other key group IO capabilities and vulnerabilities.
- The portion of the information environment in the commander's battlespace.
- The impact of the physical and information environments on friendly, adversary, and other IO.
- How adversaries and others might support their operations with IO (predictions).
- The potential impact of friendly IO on adversary and other operations (assessments).

The G-7 refines IO input to IPB throughout the operation.

PROVIDE INPUT TO THE INITIAL INTELLIGENCE, RECONNAISSANCE, AND SURVEILLANCE TASKING

5-19. Commanders deploy ISR assets as soon after they receive a mission as possible (see FM 5-0). The G-7 combines requirements for IO information, target identification, and assessments to produce IO input to the initial ISR tasking. ISR resources are limited and can be constrained by weather and other factors. Submitting IO information requirements (IRs) early increases the likelihood of obtaining information in time to affect IO execution.

5-20. The G-7 submits IO IRs to the G-2. The G-2 submits tasks for subordinate units to the G-3 and collection requests to higher headquarters. Staff members responsible for specific IO elements/related activities also submit IO IRs through their technical support channels.

PROVIDE INPUT TO THE INITIAL WARNING ORDER

5-21. The initial WARNO is the staff product for the first MDMP task. It is issued after the commander and staff have completed their initial assessment and before mission analysis begins. It includes, as a minimum, the type and general location of the operation, initial time line, and any movements or reconnaissance to begin. When they receive the initial WARNO, subordinate units begin parallel planning.

5-22. Parallel planning and collaborative planning (in units with the necessary information systems [INFOSYS]) are routine MDMP techniques. The time needed to achieve and assess IO effects makes it especially important to successful IO. Effective parallel/collaborative planning requires all echelons to fully share information as soon as it is available. Information sharing includes providing higher headquarters plans, orders, and guidance to subordinate G-7s. IO cell representatives use staff and technical channels (see FM 5-0) to share information as it is developed.

5-23. Because some IO elements/related activities require a long time to plan or must begin execution before the overall operation, WARNOs include detailed IO information. Although the MDMP includes three points at which commanders issue WARNOs, the number of WARNOs is not fixed. WARNOs serve a purpose in planning similar to that of FRAGOs during execution. Commanders issue both, as the situation requires. Possible IO input to the initial WARNO includes—

- Tasks to subordinate units for early initiation of approved IO actions, particularly for MD operations and PSYOP.
- EEFI to facilitate defensive IO and begin the OPSEC process.
- Known IO-related hazards and risk guidance.
- MD guidance and IO priorities.

PREPARE FOR SUBSEQUENT PLANNING

5-24. During the initial IO assessment, the G-7 establishes the concept of work for the IO cell. The concept of work usually includes locations, times, preparation requirements, and the anticipated schedule. Upon receiving a new mission, each planner begins gathering planning data. These can include a copy of the higher command OPLAN/OPORD, maps of the AO, appropriate references, and the IO estimate. The list of IO tools should be a part of the G-7 SOP.

5-25. The most important G-7 planning tools are the IO estimate and supporting IO element estimates (see appendix C). The IO estimate is a running estimate. The G-7 refines it and keeps it on hand throughout the operation. The IO estimate is a record of IO assessments. The G-7 uses it for planning and recommending changes throughout preparation and execution.

INITIAL TIME ALLOCATION

5-26. Based on the commander's time allocation, the G-7 allocates time to plan and prepare for IO. This allocation of available time is the most important task the G-7 performs during receipt of mission. It determines how the G-7 manages IO planning throughout the rest of the MDMP. Depending on the situation, assembling an IO cell with staff members representing each IO element facilitates IO planning and makes the best use of time. Spreading the workload among IO element representatives also helps synchronize their efforts and identify problems early.

5-27. Initial time allocation is also important to IO because some IO activities need a long time to produce effects or a significant time to assess them. The time available may be a limiting factor for some IO. The G-7 identifies IO activities for which this is the case and includes the effects of not being able to conduct (plan, prepare, execute, and assess) them in estimates and recommendations.

PLANNING IN TIME-CONSTRAINED CONDITIONS

5-28. The commander determines when to execute a time-constrained MDMP. Under time-constrained conditions, the G-7 relies on existing tools and products, either their own or those of higher headquarters. The lack of time to conduct reconnaissance requires planners to rely more heavily on assumptions and increases the importance of routing combat information and intelligence to the people who need it. A current IO estimate is essential to planning in time-constrained conditions.

SUMMARY OF RECEIPT OF MISSION ACTIONS

5-29. How well the G-7 accomplishes the receipt of mission actions determines the effectiveness of G-7 actions throughout the rest of the MDMP. It affects the quality of the OPLAN/OPORD and possibly the success or failure of the operation. The G-7 is present and carries the current IO estimate when the commander reviews the new mission and issues initial guidance. From that point, the G-7 works closely with other coordinating staff officers and planners to synchronize IO with all aspects of the operation. Input to IPB and the initial ISR tasking is time sensitive. Failing to meet the input deadline places the G-7 at a severe disadvantage. The G-7 planners work with the G-3 planners to include IO aspects in the initial WARNO. Early dissemination of IO-related information and requirements facilitates synchronization and parallel/collaborative planning.

SECTION III – MISSION ANALYSIS

5-30. During mission analysis, the staff defines the tactical problem and begins to determine feasible solutions. Mission analysis consists of 17 tasks. Many of them are performed concurrently. The mission analysis products are the restated mission, initial commander's intent, commander's guidance, and at least one WARNO. The G-7 ensures each of these products includes IO factors. The G-7 also provides IO input to other staff processes (such as IPB and targeting) and performs IO-specific tasks. The major G-7 mission analysis products are the initial IO mission statement and an updated IO estimate. Some IO objectives may also emerge. For the G-7, mission analysis focuses on developing information for use during the rest of the operations process.

5-31. The staff performs the following tasks during mission analysis:

- Analyze the higher headquarters order.
- Conduct IPB.
- Determine specified, implied, and essential tasks.
- Review available assets.
- Determine constraints.
- Identify critical facts and assumptions.
- Conduct risk assessment.
- Determine initial commander's critical information requirements.
- Determine the initial ISR annex.
- Plan use of available time.
- Write the restated mission.
- Conduct a mission analysis briefing.
- Approve the restated mission.
- Develop the initial commander's intent.
- Issue the commander's guidance.
- Issue a WARNO.
- Review facts and assumptions.

ANALYZE THE HIGHER HEADQUARTERS ORDER

5-32. Mission analysis begins with a thorough examination of the higher headquarters OPLAN/OPORD in terms of the commander's initial guidance. By examining higher echelon IO plans, commanders and staffs learn how higher headquarters are using IO elements/related activities and which IO resources and higher headquarters assets are available. The G-7 researches to understand the—

- Higher commander's intent and concept of operations.
- Higher headquarters AO, mission/task constraints, acceptable risk, and available IO assets.
- Higher headquarters schedule for conducting the operation.
- Missions of adjacent units.

Conducting IO without considering these factors may decrease IO effectiveness, increase the chance of failure, and reduce the impact of IO at all echelons. A thorough analysis also helps determine if it is necessary to request external IO support. There is no formal IO product for this task. Its purpose is for all to obtain a clear understanding of the mission and information relating to it, especially the higher commander's intent. Any questions should be raised immediately and any confusion resolved.

CONDUCT INTELLIGENCE PREPARATION OF THE BATTLEFIELD

5-33. During mission analysis, the G-2 prepares a new IPB or updates existing IPB products and the initial IPB performed upon receipt of the mission. The G-2, with technical assistance and input from other staff elements, uses IPB to define the battlefield environment, describe the battlefield's effects, evaluate adversaries, and determine adversary COAs (see FM 34-130). Figure 5-2, page 5-10, lists possible IO-related factors to consider during each IPB step. During IPB, the G-7 works with the G-2 to determine adversary IO capabilities and vulnerabilities.

- ***Information operations capabilities*** **are units or systems that support the accomplishment of information operations tasks.**
- ***Information operations vulnerabilities*** **are deficiencies in protective measures that may allow an adversary to use information operations capabilities against friendly information systems or command and control systems**.

5-34. IPB often begins with doctrinal templates that portray how adversaries may use forces and assets unconstrained by the environment. Doctrinal templates are often developed before deployment. The G-2 and G-7 may add factors from the information environment to a maneuver-based doctrinal template, or they may prepare a separate IO doctrinal template (see figure 5-3, page 5-11). Since IO often follow logical lines of operations (see FM 3-0), a separate IO template may be needed. However, when adversaries have IO assets that maneuver with their forces, adding these assets to the maneuver-based doctrinal template may be appropriate. The situation, available information, and type of adversary affect the approach taken. IO-related portions of IPB products become part of paragraph 2b of the IO estimate (see figure B-5, page B-9 and appendix C).

Define the Battlefield Environment

- Portions/aspects of the information environment that can affect friendly operations
- Features/activities that can influence information and C2 systems
- Political and governmental structures and population demographics
- Major cultures, languages, religions, and ethnic groups
- Civilian communication and power infrastructures
- Nonstate actors: NGOs and significant nonadversary groups

Describe the Battlefield's Effects

- Information environment effects on decisionmakers, C2 systems, and decisionmaking processes
- How the information environment relates to the battlefield environment
- Information environment effects on friendly, adversary, and other operations
- Combined effects of friendly, adversary, and other INFOSYS and C2 systems on the information environment and AO
- Effects of terrain, weather, and other characteristics of the AO on friendly and enemy INFOSYS and C2 systems

Evaluate the Threat

- Adversary and other group C2 systems, including functions, assets, capabilities, and vulnerabilities (both offensive and defensive)
- Assets and functions (such as, decisionmakers, C2 systems, and decisionmaking processes) that adversaries and others require to operate effectively
- Adversary capabilities to attack friendly INFOSYS and defend their own
- Models of adversary and other group C2 systems
- IO-related strengths, vulnerabilities, and susceptibilities of adversaries and other groups

Determine Threat COAs

- How adversaries and other groups may pursue information superiority
- How, when, where, and why (to what purpose) adversaries and other groups will use IO capabilities to achieve their likely objectives

Figure 5-2. Information-Operations-Related Factors to Consider During IPB

5-35. The G-7 provides input to help the G-2 develop IPB templates, databases, and other products that portray information about adversary and other key groups in the AO and area of interest. These products contain information about each group's leaders and decisionmakers. Information relevant to conducting IO includes—

- Religion, language, and culture of key groups and decisionmakers.
- Agendas of nongovernmental organizations.
- Size and location of adversary/other forces and assets.
- Military and civilian communication infrastructures and connectivity.
- Population demographics, linkages, and related information.

- Location and types of radars, jammers, and other noncommunication INFOSYS.
- Audio, video, and print media outlets and centers, and the populations they service.
- C2 vulnerabilities of friendly, adversary, and other forces/groups.

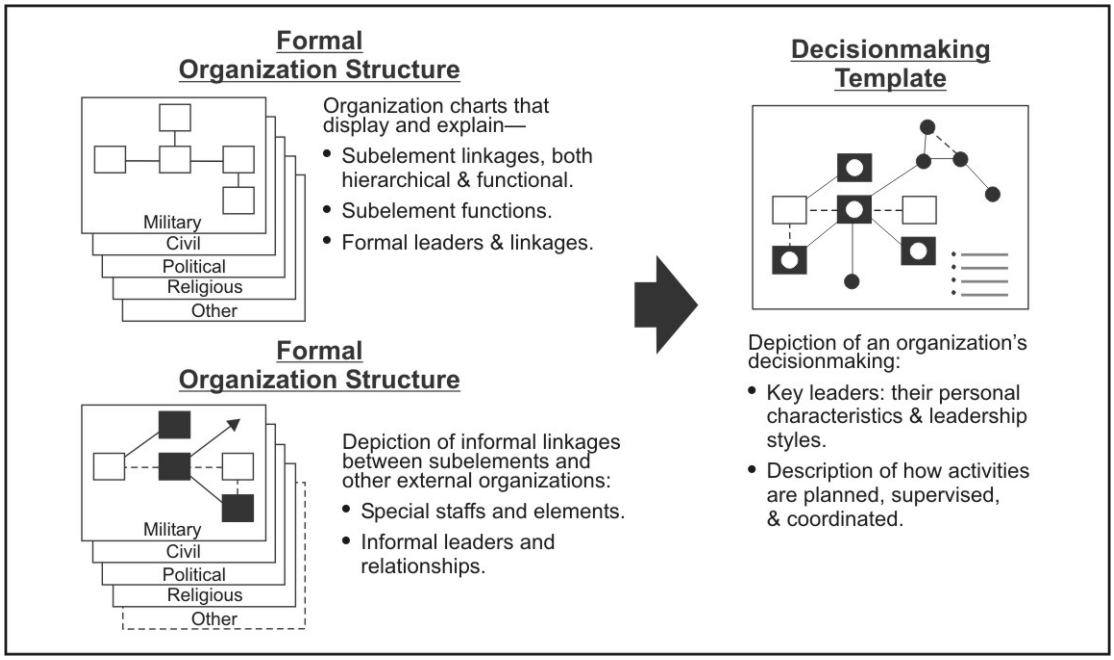


Figure 5-3. Sample Information Operations Doctrinal Template

5-36. The G-2 uses IPB to determine possible adversary COAs and arrange them in probable order of adoption. These COAs, depicted as situation templates, include adversary IO capabilities. A comprehensive IPB addresses adversary offensive and defensive IO capabilities and vulnerabilities. An IO situation template depicting how adversaries and others may employ IO capabilities to achieve information superiority is sometimes appropriate.

DEFINING THE INFORMATION ENVIRONMENT

5-37. Although the information environment has always affected military operations, its impact today is greater than ever. The G-7 brings IO IRs that address how information environment factors might affect operations to the G-2. The G-2 obtains the information from strategic and national-level databases, country studies, ISR assets, and—when necessary—other intelligence agencies.

5-38. As part of defining the battlefield environment, the G-2 establishes the limits of area of interest. The area of interest includes areas outside the AO that are occupied by adversary or other forces/groups that can affect mission accomplishment. It also includes portions of the information environment that affect operations within the AO. The ability of actors in the information environment to affect operations makes areas of interest larger than in the

past. The G-7 ensures the G-2 considers factors in the information environment when determining the area of interest. IPB includes analyzing portions of the information environment within the area of interest.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD SUPPORT OF TARGETING

5-39. IPB supports the targeting process by identifying high-value targets (HVTs) and showing where and when they may be anticipated (see appendix E). Some of these are IO-related targets. IO elements/related activities focus on different types of targets. For example, physical destruction targets are normally point targets, while PSYOP targets may be different civilian populations spread throughout the AO. The G-2 works with the G-7 to develop IO-related HVTs. The G-7 determines which IO-related HVTs contribute to one or more IO objectives and develops them as IO tasks during COA development and analysis. These tasks/targets are submitted to the targeting team as high-payoff targets (HPTs) after COA analysis.

OTHER INTELLIGENCE PREPARATION OF THE BATTLEFIELD PRODUCTS

5-40. IPB identifies facts and assumptions concerning adversaries and the operational environment that the G-7 considers when planning IO. These are incorporated into paragraph 2 of the IO estimate. The G-7 submits IO IRs to update facts and verify assumptions. Working with the G-2 and other staff sections, the G-7 ensures IO IRs are clearly identified and requests for information (RFIs) are submitted to the appropriate agency when necessary. IPB may generate priority intelligence requirements (PIRs) pertinent to IO. The G-7 may nominate these as commander's critical information requirements (CCIR) (see FM 3-0; FM 6-0). It may also identify OPSEC vulnerabilities. The G-7 analyzes these to determine appropriate OPSEC measures (see chapter 3).

DETERMINE SPECIFIED, IMPLIED, AND ESSENTIAL TASKS

5-41. Concurrently with IPB, the staff determines specified, implied, and essential tasks the unit must perform. For the G-7, this task comprises identifying IO-related specified tasks in the higher headquarters OPLAN/OPORD, developing IO-related implied tasks that support accomplishing the mission, and assembling the critical asset list (see figure B-6, page B-11). All these products are refined throughout the MDMP, based on continuous assessment of the friendly and adversary situations. The IO-related tasks identified form the basis for the initial IO mission. The G-7 develops them into IO objectives during COA development.

IDENTIFYING INFORMATION-OPERATIONS-RELATED SPECIFIED TASKS

5-42. The G-7 looks for specified tasks that may involve IO in the higher headquarters OPLAN/OPORD. Sections of the OPLAN/OPORD that may include these tasks include the commander's intent, concept of operations, air tasking order, and various annexes and operation overlays. In reviewing the higher headquarters OPLAN/OPORD for IO-related tasks, the G-7 pays particular attention to—

- Paragraph 1, Situation.
- Paragraph 2, Mission.

- Paragraph 3, Execution, especially subparagraphs on IO, tasks to maneuver units, tasks to combat support units, and CCIR.
- Annexes that address intelligence, operations, fire support, rules of engagement, IO, civil-military operations (CMO), and public affairs (PA).

5-43. Some IO-related specified tasks, such as support the higher headquarters deception plan, become unit IO objectives. Others, particularly those that address only one IO element, are incorporated under unit IO objectives as IO tasks. If the command must accomplish an IO-related task to accomplish its mission, that IO-related task is an essential task for the command.

DEVELOPING INFORMATION-OPERATIONS-RELATED IMPLIED TASKS

5-44. As the staff identifies specified and implied tasks for the overall operation, the G-7 identifies IO-related tasks that can support accomplishing them. These are IO-related implied tasks. The G-7 determines them based on what the command is required to do and how IO can support doing it. The G-7 treats both types of IO-related tasks the same way. As with specified tasks, if the command must accomplish an IO-related implied task to accomplish its mission, that IO-related task is an essential task.

ASSEMBLING THE CRITICAL ASSET LIST

5-45. **The *critical asset list* is a list of intelligence, surveillance, and reconnaissance elements, and elements of the command's command and control system, whose loss or functional disruption would jeopardize mission accomplishment.** At the operational and strategic levels, this subtask includes identifying centers of gravity. Protecting critical assets and centers of gravity is an implied task for every operation. The G-7 obtains input for the critical asset list from all IO cell representatives, particularly those from the G-2, G-3, and G-6. It and the vulnerability assessment form the basis for planning defensive IO. The G-7 establishes one or more IO objectives that focus on protecting critical assets/centers of gravity.

5-46. One means to identify critical assets is a vulnerability assessment. The command's vulnerability assessment identifies aspects of the command's C2 system that require protection. Combined with the critical asset list and centers of gravity, it forms the basis for planning defensive IO. The 1st Information Operations Command (Land) (1st IOC [L]) provides information operations vulnerability assessment teams (IOVATs) to assess and enhance a commander's ability to incorporate defensive IO into operations (see appendix F). IOVATs contribute to force protection and information assurance by conducting vulnerability analyses and recommending defensive IO and countermeasures to mitigate vulnerabilities. The vulnerability assessment is continuously updated throughout an operation. Its results are recorded in paragraph 2c(6) of the IO estimate.

REVIEW AVAILABLE ASSETS

5-47. During this task, the commander and staff determine if they have the assets required to perform the specified, implied, and essential tasks. The G-7 performs this analysis to identify IO assets and IO resources:

- ***Information operations assets*** **are organic, assigned, and attached units with information operations capabilities**.
- ***Information operations resources*** **are information-operations-capable units not assigned or attached to the command, but whose capabilities are available to conduct information operations**.

5-48. The unit task organization lists IO assets. The higher headquarters OPLAN/OPORD, particularly the intelligence and IO annexes, list IO resources. The fire support annex identifies physical destruction assets that might be assigned IO-related targets. The air tasking order shows the availability of joint air assets available for executing missions to support Army IO. If the command needs additional IO assets or IO resources, the G-7 identifies the requirements to the G-3, who coordinates with higher headquarters for them.

5-49. Identifying and obtaining IO resources allows the command to increase IO-related combat power. Some IO resources may be available to directly support the command's IO concept of support. These resources may be employed in a fashion similar to close air support. In other cases, nesting the command's IO with higher headquarters IO and synchronizing them with adjacent units' IO can create reinforcing effects, possibly for all units concerned. The IO assets of these other organizations may be considered IO resources for the command. Finally, the information environment has no boundaries. Agencies located outside the theater may be available through reachback to shape aspects of the information environment in ways that complement or reinforce the unit's IO concept of support.

5-50. The G-7 compares available IO assets and IO resources with IO-related tasks to identify capability shortfalls and additional resources required. They consider both offensive and defensive IO requirements. The specified, implied, and essential IO-related tasks form the basis for offensive IO requirements. They may include some defensive IO requirements. The critical asset list determines the minimum defensive IO requirements. The G-7 considers the following factors:

- Changes in normal task organization resulting in changed capabilities and limitations.
- Current capabilities and limitations of available units.
- Comparison of tasks to assets and capabilities.

5-51. The IO product for this task is a list of assets and resources that can be employed to execute IO. This list becomes subparagraphs 2c(2) and (3) of the IO estimate (see figure B-7, page B-12 and appendix C). G-7 personnel update this list throughout the operation. Among other things, they use it to analyze relative combat power, determine what kinds of IO tasks the command can perform, and array initial forces during COA development.

DETERMINE CONSTRAINTS

5-52. A *constraint* is a restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action the subordinate commander has for planning (FM 5-0). IO

constraints may include legal, moral, social, operational, and political factors. They may be listed in the following paragraphs or annexes of the higher headquarters OPLAN/OPORD:

- Commander's intent.
- Tasks to subordinate units.
- Rules of engagement.
- Civil military operations.
- Fire support.

Commanders may also include constraints in the commander's guidance.

5-53. Constraints establish limits within which the commander can conduct IO. They may affect the use of lethal and nonlethal fires. Constraints may also limit the use of MD and some OPSEC measures. The IO product of this task is a list of the constraints that the G-7 believes will affect the IO concept of support (see figure B-8, page B-13).

IDENTIFY CRITICAL FACTS AND ASSUMPTIONS

5-54. Sources of facts and assumptions include existing plans, the initial guidance, observations, and reports. Some facts concerning friendly forces were determined during the review of the available assets task. During IPB, the G-2, with assistance from the G-7 and other staff elements, develops facts and assumptions about adversaries and others, the AO, and the information environment. The following categories of information are important to the G-7:

- Intelligence on adversary commanders and other key leaders.
- Adversary morale.
- The weather.
- Dispositions of adversary, friendly, and other key groups.
- Available troops, unit strengths, and materiel readiness.
- Friendly force IO vulnerabilities.
- Adversary and other key group IO vulnerabilities.

5-55. The IO product of this task is a list of facts and assumptions that concern IO. Facts are placed in the subparagraph of the IO estimate that that concerns them (usually 2a, 2b, or 2c). Assumptions are placed in subparagraph 2e (see figure B-9, page B-13). The G-7 prepares and submits to appropriate agencies IO IRs for information that would confirm or disprove facts and assumptions. The G-7 reviews facts and assumptions as information is received, revising them or (for assumptions) converting them into facts.

CONDUCT RISK ASSESSMENT

5-56. Commanders and staffs assess risk when they identify hazards, (see FM 100-14) regardless of type; they do not wait until a set point in a cycle. The G-7 assesses IO-associated risk throughout the operations process. The G-3 incorporates the G-7's IO risk assessment into the command's overall risk assessment.

5-57. IO-related hazards fall into three categories:

- OPSEC vulnerabilities (hazards associated with compromise of EEFI; see chapter 3).
- C2 vulnerabilities, including those associated with the loss of critical assets (see paragraph 5-45) or identified during the vulnerability assessment (see paragraph 5-46).
- Hazards associated with executing IO tasks.

The first two categories involve tactical hazards. The last category includes both tactical and accident hazards. The G-7 uses the techniques in FM 100-14 to analyze them (See paragraphs B-15–B-17 and figure B-10, page B-14 and figure B-11, page B-15).

5-58. During mission analysis, the G-7 assesses primarily OPSEC- and C2-related hazards. The G-7 also identifies known or expected hazards from previous operations. If the higher headquarters has assigned any specified tasks, the G-7 assesses hazards associated with them as well. The G-7 assesses hazards related to executing most IO tasks during COA development and COA analysis because most IO tasks are identified then.

5-59. During mission analysis, the G-7 combines risk assessment with the OPSEC process, vulnerability assessments, and IPB products from the G-2. IPB products and the OPSEC process identify OPSEC vulnerabilities. IPB products and vulnerability assessments identify C2 vulnerabilities. After assessing the risk associated with these tactical hazards, the G-7 develops OPSEC measures and other controls, and determines residual risk. This process results in recommended OPSEC planning guidance (see paragraph 3-32) and recommended controls to protect C2 vulnerabilities. The G-7 presents these recommendations and any recommended controls for risk associated with IO-related tasks to the commander during the mission analysis briefing, or earlier if appropriate. The G-7 considers OPSEC measures and other controls the unit normally practices (SOP measures). However they are not included in this briefing. SOP measures do not require command approval. The G-3 disseminates approved OPSEC measures and other controls (other than SOP measures) by WARNO.

5-60. As do all operations, IO entail risk. Resource constraints, combined with adversary reactions and initiatives, reduce the degree and scope of information superiority possible. Risk assessment is one means commanders use to allocate resources. Staffs identify which hazards pose the greatest threat to mission accomplishment. They then determine the resources required to control them and estimate the benefits gained. This estimate of residual risk gives commanders a tool to help decide how to allocate scarce resources and where to accept risk.

DETERMINE INITIAL COMMANDER'S CRITICAL INFORMATION REQUIREMENTS

5-61. The *commander's critical information requirements* are elements of information required by commanders that directly affect decisionmaking and dictate the successful execution of military operations (FM 3-0; see also FM 6-0). CCIR include PIRs and friendly forces information requirements (FFIR). Staff sections, including the G-7, recommend CCIR to the G-3. In a time-constrained environment, the staff may collectively compile this

information. The G-3 presents a consolidated list of CCIR to the commander for approval. The commander determines the final CCIR.

5-62. Establishing CCIR is one means commanders use to focus assessment efforts. CCIR change throughout the operations process because the types of decisions required change as an operation progresses. During planning, staff sections establish IRs to obtain the information they need to develop the plan. Commanders establish CCIR that support decisions they must make regarding the form the plan takes. The most important decision during planning is which COA to select. During preparation, the focus of IRs and CCIR shifts to decisions required to refine the plan. During execution, commanders establish CCIR that identify the information they need to make execution and adjustment decisions (see FM 6-0).

5-63. During mission analysis, the G-7 determines information the commander needs to decide how to employ IO during the upcoming operation. The G-7 recommends that the commander include these IO IRs in the CCIR (see figure B-12, page B-16). This task produces no IO-specific product unless the G-7 recommends one or more IO IRs as CCIR. However, at this point, the G-7 should have assembled a list of IO IRs and submitted them to the G-2. The following is an example of CCIR for a stability operation in which an information operation is the decisive operation:

- Who are the key players in ethnic violence within the municipality?
- What is each of the political parties' platform?
- Who will represent the political parties?
- Which party is most likely to cooperate with friendly forces?
- Which party will not only represent the majority of the people, but also actively support progress within the municipality?
- What are the friendly force centers of gravity and vulnerabilities?

DETERMINE THE INITIAL INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE REQUIREMENTS

5-64. Based on the initial IPB and CCIR, the staff identifies information gaps (see FM 3-0; FM 6-0) and determines initial ISR requirements. The G-2 incorporates them into the collection plan. The collection plan is coordinated with the G-3 to ensure it includes all ground and air surveillance and reconnaissance assets. The G-3 prepares the initial ISR annex and issues the orders necessary to begin collection as soon after receipt of mission as possible.

5-65. The G-7 identifies gaps in information needed to support IO planning and to support execution and assessment of early-initiation actions. These are submitted to the G-2 as IO IRs. The G-2 incorporates them into the collection plan and the G-3 makes the appropriate ISR taskings. The IO product of this task is those IO IRs actually submitted for inclusion in the initial ISR annex.

PLAN USE OF AVAILABLE TIME

5-66. At this point, the G-3 refines the initial time plan developed during receipt of mission. The G-7 provides input specifying the long lead-time items associated with certain IO-related tasks. (Usually these involve MD or

PSYOP.) Identifying these IO-related tasks is important because of the long lead-time needed to collect and analyze intelligence, and the potentially long time necessary to achieve results. Upon receiving the revised time plan, the G-7 compares the time available to accomplish IO-related tasks with the command and adversary time lines, and revises the IO time allocation plan based on them. The IO product from this task is a revised IO time plan.

WRITE THE RESTATED MISSION

5-67. The G-3 develops the proposed restated mission based on the force's essential tasks. The G-7 provides IO input based on the current IO estimate. The restated mission must include IO-related essential tasks, if any (see figure B-13, page B-16).

CONDUCT A MISSION ANALYSIS BRIEFING

5-68. Time permitting; the staff briefs the commander on the results of its mission analysis. The mission analysis briefing is often the only time that the entire staff is present and the only opportunity to ensure that all staff members start from a single reference point. Figure 5-4 shows the topics the mission analysis briefing covers and the IO input to them. IO input is based primarily on the IO estimate. The unit SOP lists the information the G-7 provides. This information summarizes or restates the results of previous MDMP tasks and, at a minimum, captures the topics listed in figure 5-4.

Briefing Topic	Information Operations Input
Mission	• IO-related essential tasks
Initial IPB (map and display charts)	• Adversary decisionmakers, decisionmaking processes, C2 systems, IO capabilities, and IO vulnerabilities
Specified, implied, and essential tasks (text chart)	• IO-related specified, implied, and essential tasks
Constraints (text chart)	• Any constraints on IO placed on the command
Forces Available (IO asset status chart)	• Available IO assets and capabilities • Additional IO resources needed
Risk assessment (chart)	• Recommended OPSEC planning guidance • Recommended controls to protect C2 vulnerabilities and critical assets • Recommended controls for risk associated with IO-related tasks
Recommended initial CCIR (text chart)	• Information need to make critical IO decisions, especially information needed to determine or validate IO planning • Recommended IO-related CCIR
Recommended time lines (graphic display)	• Time required to accomplish IO-related tasks • Compare time needed to the time available
Recommended restated mission (text chart)	• IO-related essential tasks

Figure 5-4. Information Operations Input to Mission Analysis Briefing

APPROVE RESTATED MISSION

5-69. Following the mission analysis briefing, the commander approves the restated mission. Once approved, the restated mission becomes the unit mission. The G-7 ensures that the section members receive and understand the approved mission statement.

DEVELOP INITIAL COMMANDER'S INTENT

5-70. The *commander's intent* is a clear, concise statement of what the force must do and the conditions the force must meet to succeed with respect to the enemy, terrain, and the desired end state (FM 3-0). It links the mission with the concept of operations by stating the key tasks that, along with the mission, form the basis for subordinates to exercise initiative when unanticipated opportunities arise or when the original concept of operations no longer applies. (*Key tasks* are those tasks the force as a whole must perform, or conditions the force must meet, to achieve the end state and stated purpose of the operation [FM 6-0].) The operation's tempo, duration, and effect on the enemy or terrain that must be controlled are examples of key tasks. The G-7 develops recommended IO input to the commander's intent and submits it to the chief of staff (COS) for the commander's consideration. When developing recommended input to the commander's intent, the G-7 assists the commander in visualizing how IO can support mission accomplishment (see figure B-14, page B-17).

ISSUE THE COMMANDER'S GUIDANCE

5-71. After approving the restated mission and stating the commander's intent, the commander provides the staff with additional guidance to focus staff planning activities. The commander includes his visualization of IO in this guidance. Commanders consider the following when developing their IO planning guidance:

- Aspects of higher headquarters IO policies or guidance that the commander wants to emphasize.
- COAs for which IO is most likely to increase the chance of success.
- Risk they are willing to take with respect to IO.
- IO decisions for which they want to retain or delegate authority.

5-72. The commander's guidance focuses on the command's essential tasks (see FM 5-0). Commanders may give guidance for IO separately or as part of their overall guidance. They provide enough guidance for IO planning. This guidance includes any identified or contemplated IO objectives, stated in finite and measurable terms. It also includes OPSEC planning guidance (see paragraph 3-32), MD guidance (see paragraph 4-74), and targeting guidance (see paragraphs E-9–E-12). (See figure B-15, page B-17).

5-73. The G-7 helps the commander visualize offensive IO requirements and opportunities. The G-7 also provides expertise on friendly IO vulnerabilities, adversary IO capabilities, and available defensive IO measures. Considerations for the G-7 when recommending IO input for the commander's guidance include—

- The extent that the command is vulnerable to hostile IO.

- Specific IO actions required for the operation.
- The command's capability to execute specific offensive IO actions and to implement specific defensive IO measures.
- Additional information needed to conduct IO.

ISSUE A WARNING ORDER

5-74. Immediately after receiving the commander's guidance, the G-3 sends subordinate and supporting units a WARNO (see figure B-16, page B-18). The G-7 provides IO input to the G-3 for inclusion in the WARNO. This IO input includes the initial IO mission statement. It also includes the OPSEC planning guidance and MD planning guidance, if these are not already disseminated. It may include recommendations concerning—

- CCIR.
- Risk guidance.
- ISR tasks.
- Security measures.

REVIEW FACTS AND ASSUMPTIONS

5-75. Throughout an operation, the G-7 maintains a record of IO-related facts and assumptions in paragraph 2 of the IO estimate. The G-7 periodically reviews them. When a fact or assumption changes, the G-7 updates the IO estimate and assesses the effect of the change. If the change requires an adjustment of the operation, the G-7 advises the COS and G-3.

5-76. During the MDMP, the G-7 periodically reviews the IO facts and assumptions to ensure their comprehensiveness and validity based on the restated mission, the updated commander's guidance, and the initial commander's intent. The G-7 keeps current facts and assumptions in mind during COA development. IO issues are dynamic and require constant assessment throughout the operation.

SUMMARY OF MISSION ANALYSIS ACTIONS

5-77. A thorough mission analysis is critical to understanding the overall operation and determining how to achieve success. It lays the foundation for subsequent MDMP tasks. Information and products developed during mission analysis support development of the IO estimate, which underlies IO planning. As these are developed, the G-7 shares them with higher and lower echelon G-7s to facilitate parallel/collaborative planning. The initial IO mission statement provides the focus for developing IO concepts of support during COA development. The G-7 uses information in the IO estimate to complete IO portions of the OPLAN/OPORD during orders production.

SECTION IV – COURSE OF ACTION DEVELOPMENT

5-78. After the mission analysis briefing, the staff begins developing COAs for analysis and comparison based on the restated mission, commander's intent, and planning guidance. During COA development, the staff prepares

feasible COAs that integrate the effects of all combat power elements to accomplish the mission. Based on the initial IO mission statement, the G-7 develops a distinct IO concept of support, IO objectives, and IO tasks for each COA. IO cell members develop tasks that their IO elements/related activities can perform to help achieve IO objectives.

COA Development Tasks

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

5-79. The G-7 is involved early in COA development. The focus is on determining how to achieve information superiority at the critical times and places of each COA. Depending on the time available, planning products may be written or verbal. IO cell representatives assist the G-7 in considering and synchronizing all IO elements/related activities.

ANALYZE RELATIVE COMBAT POWER

5-80. *Combat power* is the total means of destructive and/or disruptive force, which a military unit/formation can apply against the opponent at a given time (JP 1-02). The elements of combat power are maneuver, firepower, leadership, protection, and information (see FM 3-0). By analyzing relative combat power, planners determine friendly and opposing force strengths and weaknesses, and determine which types and forms of operations (see FM 3-90) are feasible.

5-81. The G-7, assisted by the IO cell, ensures the staff considers information with the other elements of combat power. However, the staff does not fully integrate IO assets/resources until it arrays forces and develops COAs. In some instances, information complements the effects of other combat power elements; in others it reinforces them (see FM 3-0). Sometimes information is the most important element of combat power. Here are examples of how IO can increase friendly combat power:

- MD can influence adversary application of combat power at places and times that favor friendly operations.
- Counterpropaganda can degrade adversary propaganda by exposing lies and providing truth.
- PA operations can favorably influence domestic and foreign audiences by publicizing positive actions by US forces. PSYOP can achieve the same effect in foreign AOs.

5-82. The G-7 ensures that the staff considers IO capabilities when analyzing relative combat power. IO can be especially valuable in reducing resource expenditure by other combat power elements. For example, commanders can use electronic warfare (EW) to jam a communications node instead of using fires to destroy it.

5-83. Offensive and defensive IO contributions are often difficult to factor into numerical force ratios. With G-7 planners' support, staff planners consider the effects of IO on the intangible factors of military operations as

they assess relative combat power. Intangible factors include such things as the friction of war and the will of Army forces and adversaries. Varied approaches and methods may be used to portray IO effects. One method is to increase the relative combat power assigned to forces with IO assets. For example, strict OPSEC discipline by friendly forces increases the difficulty adversaries have in collecting information. Also, the PA officer can determine indicators of each side's vulnerabilities with respect to media coverage.

GENERATE OPTIONS

5-84. After determining feasible types and forms of operations, the staff generates options for conducting them. Commanders generally focus COA development with their planning guidance. As many feasible options as time allows are developed as COAs.

5-85. The G-7 assists the staff in considering the advantages and disadvantages IO brings to each possible COA. Some IO tasks—such as those that use fire support, intelligence, or maneuver assets—require tradeoffs with other maneuver options. An example is using maneuver forces for MD operations instead of weighting the decisive operation. The staff considers these tradeoffs when generating options and reviews them during COA analysis.

ARRAY INITIAL FORCES

5-86. The staff arrays forces to determine the forces necessary to accomplish the mission and to develop a knowledge base for making decisions concerning concepts of operations. The G-7 ensures that planners consider the impact of available IO assets/resources on force ratios as they determine the initial placements. IO assets/resources may reduce the number of maneuver forces required or may increase the COA options available. Planners consider the deception story during this step. Because aspects of it may affect unit positioning, the staff considers major elements of the deception story before developing COAs.

DEVELOP THE CONCEPT OF OPERATIONS

5-87. The concept of operations for a COA describes how the arrayed force is to accomplish the mission within the commander's intent (see figure B-17, page B-22). The G-7 develops a distinct IO concept of support and IO objectives for each COA based on the initial IO mission. With input from the IO cell, the G-7 considers what IO assets and resources can do to achieve the IO objectives. These capabilities are developed into IO tasks. The G-7 develops or refines the following IO products to support each COA the staff develops and prepare for COA analysis:

- IO concept of support.
- IO objectives.
- IO tasks to support each IO objective.
- IO input work sheets.
- IO synchronization matrix.
- IO-related target nominations.
- Critical asset list.

- Assessment of IO-associated risk.
- Criteria of success and IO IRs to support IO assessment.

INFORMATION OPERATIONS CONCEPT OF SUPPORT

5-88. IO concepts of support state how the commander will use IO to accomplish the IO mission. They are linked to and simultaneously developed with COAs for the overall operation. IO concepts of support identify IO priorities by critical event, phase, or unit and area (see figure B-18, page B-24). They focus IO effects on the COA's decisive point or on shaping operations that allow the force to mass combat power at the decisive point. As IO concepts of support are developed, the G-7 determines which IO elements/ related activities to use at points throughout the COA. The G-7 ensures that IO priorities are consistent with the commander's intent. First priority of IO support is to the decisive operation.

5-89. While synchronizing the IO concept of support and IO objectives with the overall COA, the G-7 also synchronizes them with those of higher and adjacent headquarters. Synchronization of the command's effort with higher headquarters IO masses IO effects. For example, a PSYOP program has an increased chance of success if it builds on programs of higher headquarters and nests with those of lower echelons.

INFORMATION OPERATIONS OBJECTIVES

5-90. IO objectives focus and state the purpose for performing IO tasks. They do not refer to any IO element. For example, there is no such thing as a PSYOP objective, only PSYOP tasks. An IO objective is stated in terms of the effect the commander desires. The initial IO mission statement focuses development of offensive and defensive IO objectives.

5-91. An offensive IO objective is stated in terms of only one IO effect: destroy, degrade, disrupt, deny, deceive, exploit, or influence. A well-defined IO objective specifies the desired effect, an action, a target, and a purpose for the action. Normally, offensive IO objectives are written in terms of causing an adversary to do or not do something: for example—

- Delay [the effect] Rendovan forces [the target] crossing of the Awash River for 72 hours [the action] to allow establishment of a forward operating base [the purpose].
- Deny [the effect] Rendovan insurgents' [the target] ability to create civil unrest [the action] in order to maintain a safe and secure environment for reestablishing civilian control and services [the purpose].

5-92. Defensive IO objectives are also written in terms of only one IO effect. They usually begin with such words as protect, detect, restore, or respond. They may have friendly, adversary, or other forces/groups as their target: for example, Protect [the effect] the 121st Division tactical command net and tactical local area network [the targets] from disruption [the action] to ensure effective command and control [the purpose]. The G-7 uses the critical asset list and IO vulnerability assessment to determine defensive IO objectives.

5-93. Mass and simplicity, two principles of war, are important when conducting IO. The number of IO objectives that a command can execute

depends on the resources available and the staff's ability to synchronize their actions. As the number of IO objectives grows, IO C2 requirements become more complex. Ideally, IO focuses on a few objectives selected to directly affect the COA's decisive point. Limiting the number of IO objectives reduces the chance of inadequate synchronization and keeps the number of IO tasks manageable. Assigning fewer IO tasks facilitates the commander's ability to mass IO effects. The command's ability to assess (monitor and evaluate) effects may limit the number of IO tasks it can assign.

INFORMATION OPERATIONS TASKS

5-94. When developing IO tasks, the G-7 considers all IO elements and determines, based on available assets and resources, what contributions each can make to achieve each IO objective. A single IO task may support several IO objectives, both offensive and defensive. Tasks are written with the intent of being unit mission statements. Staff officers responsible for each IO element analyze the IO tasks and, translate them into—

- Target nominations and assessment criteria. IO-related targets and assessment requirements are developed as IO tasks (see appendix E).
- Tasks to subordinate units.
- Requests for support to higher headquarters.
- Internal staff actions.

5-95. IO tasks tell a unit to do something. They always address only one IO element. The commander assigns IO tasks to units that are able and have the assets to perform them. Tasks of several IO elements/related activities may contribute to accomplishing a single IO objective. Conversely, a single IO task may support more than one IO objective (see figure 5-1, page 5-2).

INFORMATION OPERATIONS INPUT WORK SHEETS

5-96. The G-7 may use IO input work sheets to prepare for COA analysis and focus IO cell member efforts (see figures B-19–B-22, pages B-25–B-32). The G-7 prepares one work sheet for each IO objective in each IO concept of support. IO work sheets include the following information:

- A description of the COA.
- The IO concept of support.
- The IO objective.
- Information concerning IO tasks that support the IO objective, listed by IO element.
- Anticipated adversary counteractions for each IO task.
- Criteria of success for each IO task.
- Information required to assess each IO task.

5-97. The matrix format of the IO input work sheet shows how each IO element contributes to the IO objective and the IO concept of support for that COA. When completed, the work sheets help the G-7 tie together the staff products developed to support each COA. G-7 planners also use the work sheets to focus IO task development for all IO elements/related activities. They retain completed work sheets for use during COA analysis and orders production.

INFORMATION OPERATIONS SYNCHRONIZATION MATRIX

5-98. The G-7 develops an IO synchronization matrix for each COA to determine when to execute IO tasks. IO synchronization matrices show estimates of the time it takes for friendly forces to execute an IO task; the adversary to observe, process and analyze it; and the adversary to act on it. The G-7 synchronizes IO tasks with other combined arms tasks. The G-2 and G-3 time lines are used to reverse-plan and determine when to initiate IO tasks. Due to the lead time required, some IO tasks must be executed before combat and combat support tasks. Regardless of when the IO tasks start, they are still synchronized with other combined arms tasks. Many IO tasks are executed throughout an operation; some are both first to begin and last to end (see figure B-23, page B-33).

INFORMATION-OPERATIONS-RELATED TARGET NOMINATIONS

5-99. The G-7 uses information derived during mission analysis, IPB products, and the high-value target list (HVTL) to nominate IO-related high-payoff targets (HPTs) for each friendly COA. HPTs are selected from the HVTL and become the high-payoff target list (HPTL). IO-related HPTs are developed as IO tasks. Targets attacked by nonlethal means, such as jamming or PSYOP broadcasts, may require assessment by means other than those normally used in battle damage assessment. The G-7 submits IO IRs for this information to the G-2 when nominating them. If these targets are approved, the IO IRs needed to assess the effects on them become PIRs that the G-2 adds to the collection plan. If the command does not have the assets or resources to answer the IO IRs, the target is not engaged unless the attack guidance (see appendix E) specifies otherwise or the commander so directs. The targeting team performs this synchronization.

CRITICAL ASSET LIST

5-100. The G-7 reviews the critical asset list and centers of gravity developed during mission analysis to determine defensive IO tasks for each COA. Critical assets may be added or deleted from the list based on how their loss or degradation would affect the COA.

ASSESSMENT OF INFORMATION-OPERATIONS-ASSOCIATED RISK

5-101. The assessment of IO-associated risk during COA development and COA analysis focuses primarily on hazards related to executing IO tasks (see paragraphs B-39–B-41). However, the G-7 assesses all hazards as they emerge. The G-7 also monitors identified hazards and evaluates the effectiveness of controls established to counter them.

5-102. The G-7 examines each COA and its IO concept of support to determine if they contain hazards not identified during mission analysis. The G-7 then develops controls to manage these hazards, determines residual risk (using the procedure described in paragraphs B-14–B-17 and figures B-10 and B-11, pages B-14 and B-15), and prepares to test the controls during COA analysis (see FM 100-14). The G-7 coordinates controls with other staff sections as necessary. Controls that require IO tasks to implement are added to the IO input work sheet for the COA.

5-103. The G-7 considers two types of tactical and accident hazards associated with performing IO tasks:

- Those associated with the IO concept of support itself.
- Those from other aspects of the concept of operations that may affect execution of IO.

The G-7 identifies as many of these hazards as possible so the commander can consider them in decisions.

5-104. Some hazards result from the need to focus IO efforts. These hazards require commanders to take calculated risks (see FM 3-90). Some examples:

- As part of a MD operation, the commander limits camouflage, concealment, and deception measures applied to elements he wants the adversary to detect. The commander accepts the risk of adversaries targeting these elements.
- The commander concentrates information assurance efforts on a few critical C2 nodes, accepting the risk that other nodes may be degraded.
- The commander elects to destroy an adversary communications node that is also a valuable intelligence source. The commander accepts the risk of operating without that intelligence.

5-105. Hazards can also result from unintended actions by adversary and other forces/groups in response to friendly IO. In addition, unintended consequences of other tactical activities can affect IO. For example—

- An electronic attack may disrupt friendly as well as adversary communications (information fratricide).
- In a peace operation, influencing a mayor to support US forces instead of simply not opposing them may boost the popularity of an anti-US rival, risking loss of long-term local political support.

Thorough planning can reduce, but will never eliminate, unintended consequences. The G-7 identifies possible unintended consequences and focuses on those most likely to affect mission accomplishment.

5-106. Since adverse effects of military operations on the environment and civilians can influence IO, the G-7 considers the effects of IO-related hazards on the local populace and infrastructure as well as on friendly forces. The G-7 assesses these hazards, develops controls, determines residual risks, and advises the commander on risk mitigation measures (see figure B-24, page B-34).

5-107. The commander alone accepts or rejects risk. The G-7 advises the commander concerning risk associated with IO-related hazards and recommends IO tasks as controls to mitigate it. The commander decides what risk to accept. An example of using IO for accident risk mitigation is the integrated use of CMO, PSYOP, and PA to warn the local populace of the accident hazards associated with military operations. When appropriate, the G-7 converts risk mitigation measures into IO tasks. These are assigned to units or placed in the IO annex coordinating instructions. Risk control measures that apply to the entire force are placed in the OPLAN/OPORD coordinating instructions.

5-108. The G-7 produces a list of IO-related hazards and assessments of their associated risks. This list becomes the IO input to the G-3 risk assessment matrix (see figure B-10, page B-14, and figure B-24, page B-34).

CRITERIA OF SUCCESS AND ASSESSMENT

5-109. *Criteria of success* are information requirements developed during the operations process that measure the degree of success in accomplishing the unit's mission. They are normally expressed as either an explicit evaluation of the present situation or forecast of the degree of mission accomplishment (FM 6-0). As COA development continues, the G-7 considers how to assess IO effectiveness. The G-7 determines—

- IO tasks that require assessment.
- Preliminary criteria of success for each IO task, including IO-related targets.
- The information needed to make the assessment.
- How to collect the information.
- Who will collect the information.
- How the commander will use the information to support decisions.

These are recorded on IO input work sheets and added to the IO assessment matrix during orders production (see figure B-26, page B-39). The effects of IO tasks must be measurable in terms of criteria of success. The G-7 identifies information required to determine whether each IO task has met its criteria of success, the possible sources of required information, and the means available to obtain the information. The G-7 pays particular attention to IO-related targets nominated for nonlethal engagement, since most require information gathered by ISR assets to assess. Criteria of success for defensive IO tasks are expressed in terms of *protect* or other appropriate term. FM 7-15 lists measures of effectiveness for IO tasks that the G-7 may use as examples of criteria of success. The G-7 's challenge is to develop criteria of success that will help assess the overall effectiveness of IO execution (see paragraphs 6-25—6-32).

5-110. Information required for the G-7 to assess IO effects becomes IO IRs. The G-7 submits IO IRs for the COA the commander approves to the G-2. The G-7 establishes criteria of success based on how each task's effects contribute to achieving one or more IO objectives. If a task's results are not measurable, the G-7 eliminates the task.

5-111. Assessing all tasks during execution may be impractical. At a minimum, IO tasks that support the decisive operation are assessed. The G-7 works with the G-2 to include IO IRs that support assessment in the collection plan and the appropriate sections of the OPLAN/OPORD. (See figure B-26 for an example of an IO assessment matrix.)

RECOMMEND HEADQUARTERS

5-112. For each COA, the staff recommends headquarters to command and control the forces available to execute it. When approved, these assignments become the task organization. The G-7 identifies units to perform IO tasks and makes task organization recommendations based on IO factors.

5-113. When developing IO objectives and tasks, the G-7 organizes IO tasks by IO element. However, IO elements are not organizations. For an IO task to be performed, it must be assigned to a unit. The G-7 recommends units to perform each IO task. These recommendations take into account tradeoffs

between using units to apply the information versus other elements of combat power. They are refined during COA analysis.

5-114. The G-7 makes task organization recommendations based on the IO capabilities of each headquarters, IO assets assigned and IO resources attached to it. The IO estimate, including the vulnerability assessment, provides information needed to support any IO-related recommendations. For example, a headquarters inexperienced in using the latest INFOSYS should not be assigned to a critical role in an operation where the adversary force is highly capable of electronic attack. Likewise, a headquarters highly capable in using INFOSYS may be ideal to oppose an adversary with a cumbersome, low technology, or inexperienced decisionmaking capability. Another consideration is the headquarters' experience in conducting IO. The G-7's consideration of each headquarters' vulnerabilities may result in additional defensive IO tasks.

PREPARE COURSE OF ACTION STATEMENTS AND SKETCHES

5-115. The G-3 prepares a COA statement and supporting sketch for each COA for the overall operation. Together, the statement and sketch cover who, what, when, where, how, and why for each subordinate unit. They also state any significant risks for the force as a whole. The G-7 provides IO input to each COA statement and sketch. At a minimum, each COA statement or sketch should include the IO concept of support. This statement may identify the most important IO objectives and IO tasks for the COA (see figure B-17, page B-22).

5-116. The G-7 may prepare an IO concept of support sketch for each COA. IO synchronization matrices may serve as these sketches. They can be used to depict the IO concept of support to IO cell members or as a briefing aid. They may be based on logical lines of operations.

SUMMARY OF COA DEVELOPMENT TASKS

5-117. At the end of COA development, the G-7 has a synchronized IO concept of support, IO objectives, and IO tasks for each COA. The G-7 knows which units will perform each task, where they need to be at the execution time, and when the task is to be executed. Criteria of success and the source of the information required to assess each task are identified. The G-7 has organized this information for COA analysis using IO input work sheets, IO concept of support sketches, synchronization matrices, or other products.

SECTION V – COURSE OF ACTION ANALYSIS (WAR-GAMING)

5-118. COA analysis (war-gaming) identifies which COA accomplishes the mission with minimum casualties while best positioning the force to retain the initiative. War-gaming is a disciplined process that staffs use to envision the flow of battle. Its purpose is to stimulate ideas and provide insights that might not otherwise be discovered. Effective war-gaming allows the staff to test each COA, identify its strengths and weaknesses, and alter it if necessary. During war-gaming, new hazards may be identified, the risk associated

with them assessed, and controls established. OPSEC measures and other risk control measures are also evaluated.

5-119. War-gaming helps the G-7 synchronize IO element/related activity effects and helps the staff integrate IO into the overall operation. During the war game, the G-7 addresses how each element/related activity contributes to the IO concept of support for that COA and its associated time lines, critical events, and decision points. The G-7 revises IO concepts of support as needed during war-gaming.

5-120. The G-7 uses IO execution matrices and IO input work sheets for each COA as scripts for the war game. The IO elements/related activities are synchronized with each other and with the concepts of operations for the different COAs. To the extent possible, the G-7 also includes planned IO counteractions to anticipated adversary reactions.

5-121. During preparation for war-gaming, the G-7 gives the G-2 likely adversary IO actions and reactions to friendly IO. The G-7 also continues to provide input to the G-2 for HPT development and selection.

5-122. Before beginning the war game, staff planners develop evaluation criteria to measure the effectiveness and efficiency of each COA. They use these to compare COAs during COA comparison. These criteria are listed in paragraph 2c(5) of the IO estimate and become the outline for the COA analysis subparagraphs of paragraph 3 (see appendix C). The G-7 develops the criteria for evaluating IO concepts of support. Using IO-specific criteria allows the G-7 to explain the IO advantages and disadvantages of each COA. IO evaluation criteria that may help discriminate among various COAs could include—

- Lead time required for IO implementation.
- How often information superiority must be achieved for the COA to succeed.
- The number of decision points that require IO support.
- The cost of IO versus the expected benefits.
- The risk to friendly assets posed by adversary IO.

5-123. During war-gaming, the G-7 participates in the action-reaction-counteraction process. For example, the IO action may be EW jamming; the adversary reaction may be changing frequencies; the IO counteraction may be jamming the new frequency. The G-7 uses the IO execution matrices and IO input work sheets to insert IO tasks into the war game at the time planned. A complete IO input work sheet allows the G-7 to state the organization performing the task and its location. The G-7 remains flexible throughout the process and is prepared to modify input to the war game as it develops. The G-7 is also prepared to modify the IO concept of support, IO objectives, and IO tasks to counter possible adversary actions discovered during the war game. The G-7 notes any branches and sequels identified during the war game. Concepts of support for them are developed as time permits.

5-124. The results of COA analysis are a refined IO concept of support and associated products for each COA. During war-gaming, the G-7 refines IO IRs, IO-related EEFI, and HPTs for each COA, synchronizing them with that COA's concept of operations. Staff planners normally record war-gaming

results, including IO results, on the G-3 synchronization matrix. The G-7 may also record the results on IO input work sheets. These help the G-7 synchronize IO element efforts. These matrices provide the basis for IO input to paragraph 3 of the OPLAN/OPORD, paragraph 3 of the IO annex, and IO element appendixes (see appendix D).

SECTION VI – COURSE OF ACTION COMPARISON

5-125. During COA comparison, the staff compares feasible courses of action to identify the one with the highest probability of success against the most likely adversary COA and the most dangerous adversary COA. Each staff section evaluates the advantages and disadvantages of each COA from the staff section's perspective, and presents its findings to the staff. The staff outlines each COA in terms of the evaluation criteria established before the war game and identifies the advantages and disadvantages of each with respect to the others. The G-7 records this analysis in paragraph 4 of the IO estimate (see appendix C).

5-126. The G-7 determines the COA that IO can best support based on the evaluation criteria established during war-game preparation. The results of this comparison become paragraph 5 of the IO estimate.

SECTION VII – COURSE OF ACTION APPROVAL

5-127. After completing the COA comparison, the staff identifies its preferred COA and recommends it to the commander—in a COA decision briefing, if time permits. The concept of operations for the approved COA becomes the concept of operations for the operation itself. The IO concept of support for the approved COA becomes the IO concept of support for the operation. Once a COA is approved, the commander refines the commander's intent and issues additional planning guidance. The G-3 then issues a WARNO and begins orders production (see figure B-25, page B-36).

5-128. The WARNO issued after COA approval contains information that executing units require to complete planning and preparation. Possible IO input to this WARNO includes—

- IO contributions to the commander's intent/concept of operations.
- Changes to the CCIR.
- Additional or modified risk guidance.
- Time-sensitive reconnaissance tasks.
- IO tasks requiring early initiation.
- A summary of the IO concept of support and IO objectives.

5-129. During the COA decision briefing, the G-7 is prepared to present the associated IO concept of support for each COA and comment on the COA from an IO perspective. If the G-7 perceives the need for additions or changes to the commander's intent or guidance with respect to IO, he asks for it.

SECTION VIII – ORDERS PRODUCTION

5-130. Based on the commander's decision and final guidance, the staff refines the approved COA and completes and issues the OPLAN/OPORD. Time permitting, the staff begins planning branches and sequels. The G-7 ensures IO input is placed in the appropriate paragraphs of the base order and its annexes (see figure 5-5). If the OPLAN/OPORD requires an IO annex, the G-7 prepares it. The IO annex usually includes an IO execution matrix and an IO assessment matrix as appendixes. When necessary, the G-7 or appropriate special staff officers prepare appendixes for one or more IO elements/related activities.

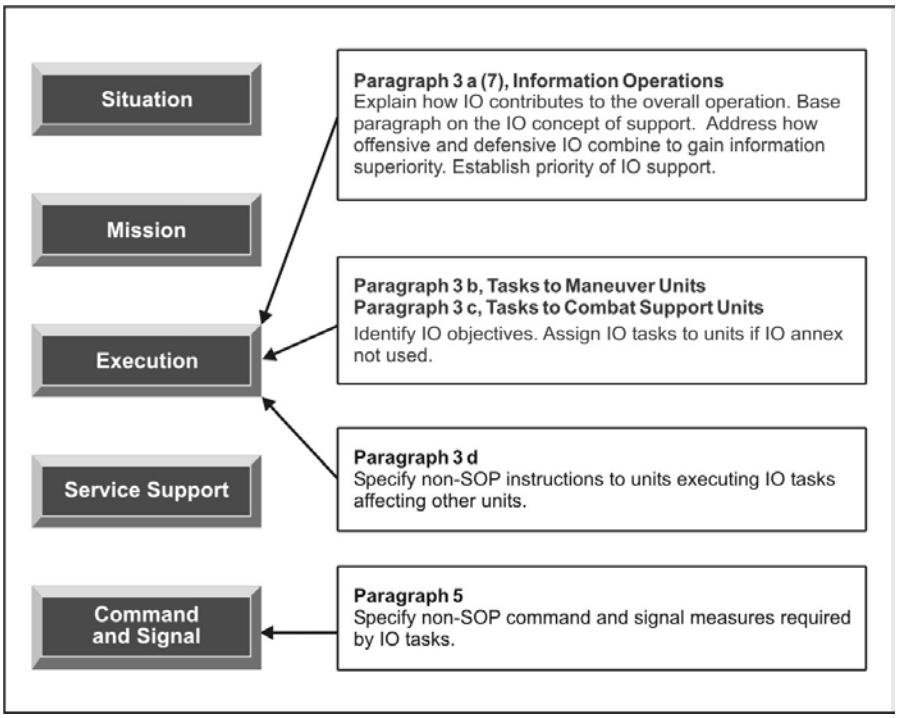


Figure 5-5. Information Operations Input to the Base OPLAN/OPORD

G-7 ACTIONS ON COURSE OF ACTION APPROVAL

5-131. With approval of a COA, the IO concept of support for that COA becomes the IO concept of support for the operation. If necessary, the G-7 modifies it and other IO planning products based on the revised commander's intent and planning guidance. The G-7 refines the IO tasks to support accomplishing the finalized IO objectives. The IO synchronization matrix for the approved COA becomes the basis for the IO execution matrix for the operation.

5-132. Placement of IO tasks in the OPLAN/OPORD varies according to the importance of the task and the complexity of the operation. IO tasks may appear in the body of the order—particularly if it is relatively simple or short,

as may be the case of a FRAGO or WARNO. For complex plans and orders, only the IO concept of support and IO objectives appear in the body. IO tasks are placed under tasks to subordinate units in the IO annex, IO element appendixes, or other annexes.

INPUT TO THE OPERATION PLAN/OPERATION ORDER

5-133. The G-7 writes paragraph 3a(7) of the base OPLAN/OPORD, which discusses IO, and the IO annex. Paragraph 3a(7) states the IO concept of support and IO objectives. If an IO annex is not used, it may contain a subparagraph for each IO element/related activity and follow the same format as paragraph 3 of the IO annex (see appendix D). Paragraph 3a(7) establishes priority of support and refers to appropriate annexes and IO element appendixes as required. This paragraph gives the staff and subordinate commands the information needed to synchronize IO effects.

5-134. IO-related reporting requirements appear in the OPLAN/OPORD coordinating instructions. IO tasks are placed in the coordinating instructions in the following circumstances:

- When an IO task affects two or more units.
- When the timing of an IO task depends on friendly actions.
- When the task involves synchronization with fire support and EW actions.

SUMMARY OF ORDERS PRODUCTION

5-135. Orders production is the last step of the MDMP. Its product is a complete OPLAN/OPORD with supporting documents. When the time comes to write input to the body of the order and the IO annex, nearly all the detailed coordination, synchronization, and deconfliction work is completed. The G-7 coordinates the IO annex with organizations involved with executing tasks and with those IO will affect. The G-7 also crosswalks the IO annex with the OPLANs/OPORDs of higher, lower, and adjacent units. During planning, the force has made some preparations for the operation based on WARNOs and the results of parallel and collaborative planning. When the OPLAN/OPORD is issued, the force focuses its efforts on preparing for the operation.

Chapter 6

Preparing for Information Operations

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

PREPARATION CONCEPTS

6-1. Preparation is an activity of the operations process (see FM 3-0; FM 6-0). Most preparations occur between receipt and execution of an operation order (OPORD); however, preparation begins during planning and often continues during execution. For example, a unit assigned a reserve or striking-force mission prepares until the commander commits it. When a unit executing one mission receives a warning order (WARNO) for a follow-on mission, it begins preparing for that mission, while executing its current mission.

6-2. Because many information operations (IO) objectives and IO tasks require long lead times to create the desired effects, preparation for IO often starts earlier than for other types of operations. Initial preparation for specific IO elements may begin during peacetime, although execution is during conflict or war. Peacetime preparation by units involves building contingency plan databases about the anticipated area of operations (AO). These databases can be used for IO input to IPB and to plan defensive IO, such as network protection and operations security (OPSEC). IO portions of

CONTENTS

contingency plans are continuously updated. Normal IO cell participants maintain their own data to provide the G-7 with the latest information. Peacetime preparation also lays the groundwork for IO coordination in operational and tactical units.

6-3. During peacetime, the G-7 prepares for future operations by analyzing potential target countries' IO capabilities. Examples of factors to consider include—

- Religious, ethnic, and cultural mores, norms, and values.
- Communications infrastructure.
- Military communication and C2 infrastructure.
- Military training and level of proficiency (to determine susceptibility to denial, deception, and psychological operations [PSYOP]).
- Literacy rate.
- Ethnic factional relationships and languages.

6-4. Preparation includes assessing unit readiness to execute IO. Commanders and staffs monitor preparations and evaluate them against criteria of success established during planning to determine variances. (See FM 6-0.) This assessment forecasts the effect of those factors on readiness to execute the overall operation as well as individual IO tasks.

6-5. Preparation for IO takes place at three levels: G-7, units assigned IO tasks, and individual. The G-7 helps prepare for IO by performing staff tasks and monitoring preparations by units assigned IO tasks. These units perform preparation activities as a group for tasks that involve the entire unit, and as individuals for tasks that each soldier and leader must complete.

6-6. While many IO tasks are not executed until the overall operation begins, some start while the unit as a whole is preparing for the operation. Most defensive IO tasks are executed continuously. This situation requires units assigned IO tasks to plan and prepare very quickly. A complete IO estimate based on current relevant information is necessary. Technical competence and leadership are essential to success.

REVISE AND REFINE PLANS AND ORDERS

6-7. Plans are not static; the commander adjusts them based on new information. This information may include assessments of unit preparations or answers to IO information requirements (IRs). While Army forces are preparing, adversaries also prepare and may execute their own IO. When the commander directs revising or refining the plan, the G-7 adjusts the IO portion of it.

6-8. During preparation, the G-7 adjusts the IO portions of the operation plan (OPLAN) or OPORD to reflect the commander's decisions and changes to the IO estimate. The G-7 updates the IO estimate so that it contains the most current information about adversary IO activities, changes in the weather or terrain, and friendly IO capabilities (see appendix C).

6-9. The G-7 ensures that IO input to IPB remains relevant throughout planning and preparation. To do this, he ensures that IO input to the

intelligence, surveillance, and reconnaissance (ISR) plan is adjusted to support refinements and revisions made to the OPLAN/OPORD.

6-10. IO preparation begins during planning. As the IO annex begins to take shape, G-7 coordination is vital because IO affects several battlefield operating systems. For example, planning a physical destruction attack on a command and control (C2) high-payoff target requires coordination with the targeting team (see appendix E). A comprehensive attack offering a high probability of success may involve air interdiction, deep attack, and intelligence assets. Such an IO-related target must be placed on the air tasking order. Rocket and missile fires have to be scheduled in the fire support plan. Army jammers and collectors need to fly the missions when and where needed. Making sure the different portions of the OPLAN/OPORD contain the necessary instructions requires coordination and attention to detail.

6-11. Effective IO is consistent at all echelons. The G-7 reviews subordinate unit OPLANs/OPORDs to ensure IO tasks have been effectively addressed and to detect any inconsistencies. The G-7 also looks for possible conflicts between the command's OPLAN/OPORD and those of subordinates. When appropriate, the G-7 reviews adjacent unit OPLANs/OPORDs for possible conflicts. This review allows the G-7 to identify opportunities to mass the IO effects of both units.

6-12. OPLAN/OPORD refinement includes developing branches and sequels. Branches and sequels are normally identified during war-gaming (COA analysis). However, the staff may determine the need for them at any time. The G-3 prioritizes branches and sequels. The staff develops them as time permits. The G-7 participates in their development as with any other aspect of planning (see chapter 5).

6-13. The focus during preparation for IO returns to assessment. A critical part of assessment is monitoring and evaluating the criteria of success that were developed during planning. The criteria of success for IO are monitored and refined as the plan is revised. The initial development and subsequent adjustments to the criteria of success are difficult tasks because, in many respects, establishing criteria of success is more art than science. However, a continued effort to refine criteria of success and ensure they are tied to an effective assessment process enables the G-7 to better determine the progress and effectiveness of IO, thereby enhancing IO support to the force.

ASSESSMENT OF INFORMATION OPERATIONS

6-14. Assessing the effectiveness of an information operation is one of the greatest challenges facing a staff. To assess IO effectiveness, the G-7 must quantify the intangible attributes of the information environment. The lack of physical evidence of IO effects makes this task difficult.

6-15. The *information environment* is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included, is information itself (JP 3-13). Thus, the information environment is a combination of physical assets (information systems [INFOSYS]) and nonphysical concepts (information, information-based

processes, and human decisionmaking processes). IO attack and defend the physical assets of the information environment to affect its nonphysical aspects.

6-16. Not all IO capabilities reside in the physical world. While the IO element of physical destruction is tangible, many IO elements are nonphysical. Operations security (OPSEC), some aspect of electronic warfare (EW), military deception (MD), and psychological operations (PSYOP) all aim to produce effects in the intangible domain of ideas, perceptions, and attitudes. Capturing data or information to measure such nonphysical effects is difficult and often time-consuming. It requires a depth of analysis that seems impossible during high-tempo operations.

6-17. An integrated information operation achieves a complex, tiered hierarchy of effects (see figure 6-1). Attacking or defending physical assets yields the first-order effects, such as destruction, degradation, and disruption of enemy signal nodes and command posts. First-order effects are directed against adversary INFOSYS to achieve second-order effects on adversary information and information-based processes. Effective second-order effects produce third-order effects on the enemy commander's decisionmaking. Producing these third-order effects is the ultimate goal of IO.

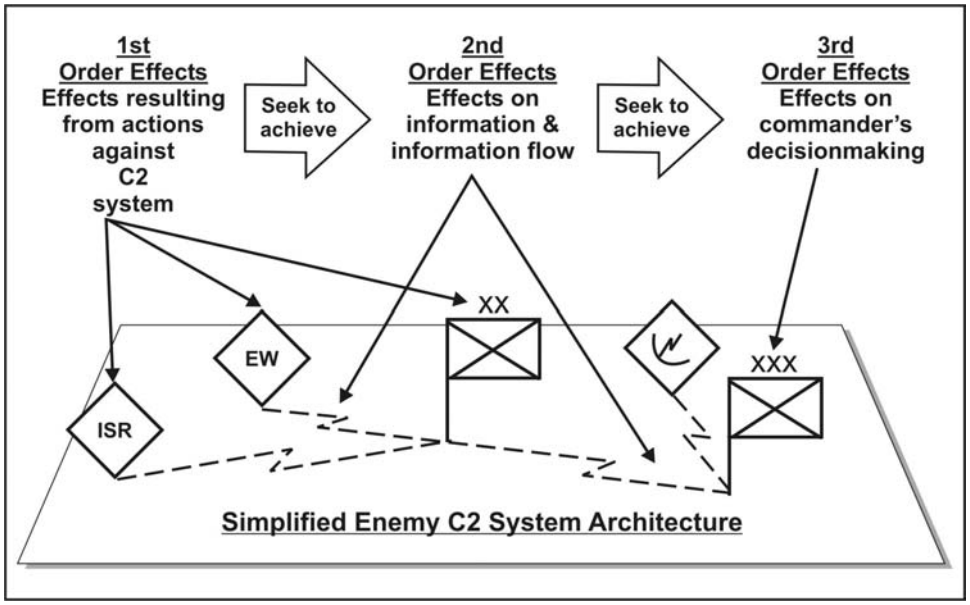


Figure 6-1. Information Operations Effects Hierarchy

6-18. Defensively, first-order effects may be the protection of friendly force INFOSYS. Second-order effects may be the maintenance of situational understanding or an uninterrupted information flow. Third-order effects may be the preservation of effective decisionmaking. Each level of effects produces corresponding enemy and friendly reactions. This situation results in a complex, tiered set of causes and effects, which must be identified and interpreted to determine the overall impact of IO. To sort through this maze of causal relationships, something more than traditional battle damage assessments (BDA) is required.

ASSESSMENT AND HIERARCHY OF EFFECTS

6-19. *Assessment* is the continuous monitoring—throughout planning, preparation, and execution—of the current situation and progress of an operation, and the evaluation of it against criteria of success to make decisions and adjustments (FM 3-0). Measurement and analysis of effects resulting from the attack of enemy INFOSYS and protection of friendly INFOSYS make assessment of IO possible. However, to do this, it is necessary to understand the hierarchy of effects resulting from IO activities (first-, second-, third-order effects).

6-20. First-order effects result from offensive IO directed against enemy INFOSYS and defensive IO taken to protect friendly INFOSYS. Generally, first-order effects are determined from reports and BDA. This level of assessment determines whether planned offensive and defensive IO tasks have occurred and the effects of them.

6-21. Second- and third-order effects are those generated by the sum total of actions directed against enemy and friendly INFOSYS. These effects are less detectable and quantifiable than first-order effects. At these levels, assessment seeks to determine if the aggregate of executed IO tasks have achieved the desired result: What were the effects on the enemy and friendly INFOSYS (second-order effects)? Were the enemy and friendly commanders affected (third-order effects)? If so, how and to what extent? Second- and third-order effects are usually determined through inductive analysis of intelligence reports and assessments.

ESTABLISHING CAUSE AND EFFECT

6-22. Because IO and the information environment are a mixture of physical assets and abstract concepts, the only way to achieve cause and effect linkages is to acknowledge that military conflict consists of interactions between humans and technology. Also, it is assumed that the physical assets of a military force and the intangible aspects of military operations, such as morale, leadership, will, and cohesion, are linked. Thus, attacking physical assets—command posts, target acquisition systems, intelligence collection and processing systems, and communication systems—will adversely impact a military force's ability to make and act upon decisions. Consequently, this will have a detrimental affect on those intangibles that provide the military force with the ability to conduct operations.

6-23. Establishing a linkage or correlation is necessary to determine whether IO elements/related activities are impacting friendly and enemy information flow and decisionmakers. A correlation exists when the value of an action (such as number of occurrences or degree of effect) increases or decreases, causing the value of the effect to increase or decrease. For example, a correlation exists in the following cases:

- The number of enemy soldiers surrendering increases after PSYOP leaflets dropped on enemy formations.
- The traffic on a C2 net decreases as the number of jamming attacks against it increase on that net.

This deductive reasoning forms the basis of determining first-order effects.

6-24. However, the relationship between action (cause) and effect may be coincidental, meaning that the occurrence of an effect is either purely accidental or perhaps caused by the correlation of two or more actions executed to achieve the effect. For example, if friendly forces are successfully engaging enemy formations with fire and maneuver at the same time PSYOP activities are urging enemy soldiers to surrender, then correlating an increase in surrendering soldiers to PSYOP activities may not be accurate. Furthermore, because IO often employ multiple elements to engage the adversary C2 system, the cumulative effect of IO support to combat actions may make the impact of individual IO objectives and tasks indistinguishable. Since there will rarely be enough time to definitively rule out coincidental relationships, the only possible antidote is an in-depth knowledge of the enemy and information environment that facilitates the development of an informed estimate through inductive reasoning.

DEVELOPING CRITERIA OF SUCCESS

6-25. *Criteria of success* are information requirements developed during the operations process that measure the degree of success in accomplishing the unit's mission. They are normally expressed as either an explicit evaluation of the present situation or forecast of the degree of mission accomplishment (FM 6-0). Criteria of success determine second- and third-order effects by establishing a cause-and-effect linkage between usually observable and quantifiable first-order effects, and abstract and subjective second- and third-order effects. Criteria of success do not constitute the assessment itself. They are an evaluation means to determine if the individual IO tasks are achieving the IO objectives and whether achieving the IO objectives is fulfilling the IO concept of support. This ensures the success of the IO mission. Criteria of success may be developed to measure the accomplishment of individual IO tasks. Doing so is largely dependent upon the importance of the task, as well as the availability of resources and time conduct an assessment to that level of detail. (See figure 6-2.)

6-26. Criteria of success are developed during planning (see chapter 5) to determine the effects of both offensive and defensive IO. To be meaningful, criteria of success must link friendly and enemy actions and activities (causes) to enemy and friendly capabilities to make and act upon decisions (effects). Therefore, criteria of success development begins with the IO mission statement. Developing effective criteria of success requires a properly crafted IO mission statement, IO concept of support, IO objectives, and IO tasks.

6-27. **The *information operations mission statement* is a short paragraph or sentence describing what the commander wants IO to accomplish and the purpose for accomplishing it.** An effective IO mission statement focuses on specific aspects of the operation. It is not a general statement that merely identifies standard doctrinal requirements for IO.

6-28. **The *information operations* concept of support is a clear, concise statement of where, when, and how the commander intends to focus the information element of combat power to accomplish the**

mission. The criteria of success developed for each of the IO objectives collectively lead to the success of the IO concept of support for the approved course of action.

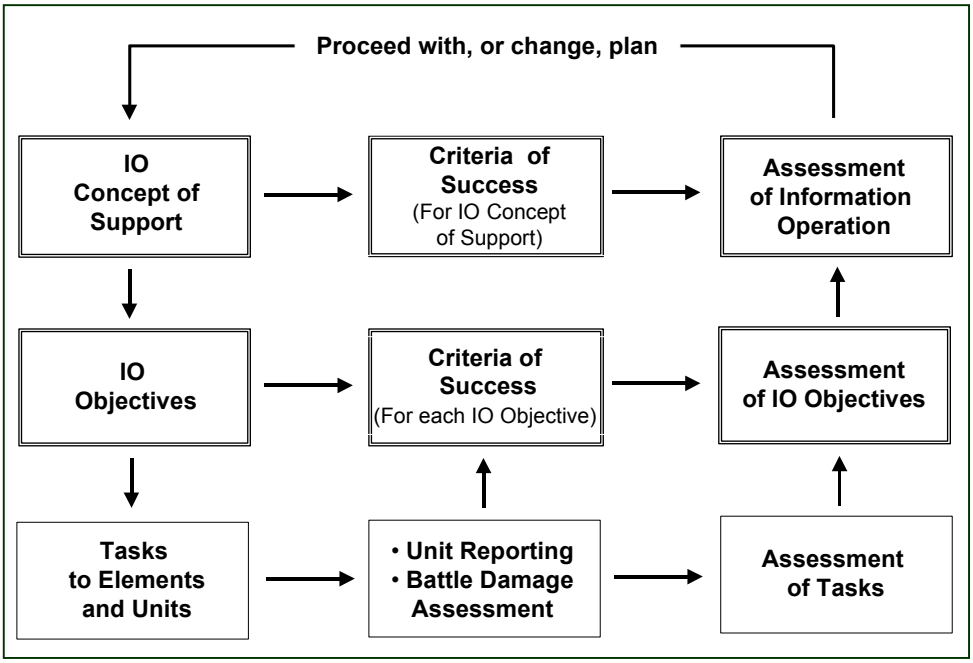


Figure 6-2. Criteria of Success in Assessing an IO Mission Statement

6-29. ***Information operations*** **objectives are clearly defined, obtainable aims that the commander intends to achieve using IO elements/related activities.** Criteria of success are developed to assess each IO objective's desired effect. A well-crafted IO objective specifies an effect, an object of the effect, and a purpose for the effect. Normally, offensive IO objectives are written in terms of destroy, disrupt, degrade, deny, deceive, exploit, and influence. Defensive IO objectives are written in terms of protecting and defending friendly force's information and INFOSYS. Ideally, each objective has a clearly defined, attainable effect. Otherwise it is not possible to determine if or when that effect is achieved, and whether the IO objective is met.

6-30. ***Information operations*** **tasks are tasks developed to support accomplishment of one or more IO objectives.** Criteria of success are stated for each task, with the understanding that an IO task addresses only one IO element/related activity. Unit reporting or BDA is important to assess the effectiveness of the individual IO task.

6-31. Criteria of success for second-order effects seek to determine if the aggregate of IO tasks are accomplishing the IO objectives. If possible, the criteria of success should be observable (to aid intelligence collection), quantifiable (to increase objectivity), precise (to ensure accuracy), and correlated to the progress of the operation (to attain timeliness). While it is

possible for an IO objective to have multiple criteria of success, limited intelligence collection and analysis assets may preclude this.

6-32. Criteria of success for third-order effects seek to determine if the enemy and friendly commanders were affected by IO as planned. These criteria of success should determine if the decisionmaker has responded as predicted. Often, these criteria of success are subjective.

ASSESSMENT – PUTTING IT ALL TOGETHER

6-33. Criteria of success are but one part of assessment. Traditional BDA and other intelligence analyses, as well as friendly unit reporting, are still key to assessing IO effectiveness. These sources provide the information on quantifiable effects. This information can be used as the basis for estimates of whether the IO mission is being accomplished. Information from unit reports and BDA are typical sources for determining first-order effects. Intelligence reporting and assessments provide information to determine second- and third-order effects.

6-34. Once criteria of success are written, a mechanism to obtain the information needed to determine the three orders of effects is developed. (See figure B-26, page B-39, for an example of an IO assessment matrix.) The G-7 determines the assessments required, specific information needed to make the assessments, and agencies and assets tasked to provide the information. This assessment plan then contributes to the command's intelligence collection plan and friendly forces information requirements (FFIR).

6-35. Timely and accurate reporting of information is essential to assessing IO effectiveness. Much of this information is reported from subordinate units. Intelligence collection assets—including maneuver units, tactical PSYOP teams, and tactical human intelligence (HUMINT) teams—all provide information with which to gauge IO mission success. Additionally, on-going intelligence analysis, including analysis of media and other open sources, supports assessing whether IO is achieving its objectives and if the IO concept of support is successful. Civil affairs tactical support teams, although not intelligence collection assets, can also provide feedback on IO mission success.

6-36. To receive information, the G-7 must actively monitor the operational situation and aggressively pursue information through unit reports and debriefings, IO cell meetings, and other venues. Commanders' battle update briefings, conference calls, and other meetings also facilitate monitoring IO execution. They provide a forum from which information is received for subsequent analysis. Some other G-7 actions are—

- Submit requests for information (RFIs) based on the assessment plan.
- Coordinate with the effects coordination cell and targeting team for BDA reporting.
- Review assessments at each IO cell meeting.
- Monitor G-2 and G-3 incident databases and analyze trends.

FORCE PROTECTION

6-37. Force protection is a continuous process executed by all commanders, regardless of the mission, location, or threat. It consists of a broad set of unit-specific, coordinated actions conducted to protect the force. Commanders conduct force protection operations throughout the range of operations (offensive, defense, stability, support) and the across the spectrum of conflict (peace, crisis, war). The G-7 develops and initiates force protection actions during planning, but executes them mainly during preparation and execution. IO actions related to force protection include tasks involving all IO elements.

6-38. Threat assessment, begun during planning, continues during the preparation. Force protection measures may include IO elements. IO conducted to support force protection is related to protecting the integrity and capability of the force. These operations may also physically protect the headquarters and communications assets. The most prominent IO elements with respect to force protection are OPSEC, (see chapter 3) physical security, counterintelligence, PYSOP, computer network defense, and information assurance (see chapter 2).

6-39. Some IO-related questions that the commander and staff may ask when preparing force protection measures are—

- Do IO rules of engagement (ROE) support force protection?
- In multinational operations, what will be the multinational ROE before hostilities and after the first hostile act?
- When will training of IO-capable units take place? at home or en route—either to operation or in the AO?
- What collective training IO-capable units take place?
- Have PSYOP been developed to support force protection?
- Have PSYOP assets been requested?

COORDINATION AND LIAISON

6-40. Synchronized operations require all units to coordinate with each other continuously. Coordinating IO begins during planning; however, input to a plan alone does not constitute coordination. Coordinating involves exchanging the information needed to synchronize operations. The majority of coordination takes place during preparation. It is then that the G-7 follows up on the coordination made during planning. Exchanging information is critical to successful coordination and execution. Coordination may be internal or external. Liaison is an important coordination means (see FM 6-0).

INTERNAL COORDINATION

6-41. Internal coordination occurs within the unit headquarters. The G-7 initiates the explicit and implicit coordinating activities within itself and with other staff sections. Much of this coordination occurs during IO cell meetings; however, IO cell members do not wait for a meeting to coordinate. They remain aware of actions that may affect, or be affected by, their

functional responsibilities. They initiate coordination as soon as they become aware of a situation that requires it. The G-7 remains fully informed of IO-related coordination. The G-7 corrects or resolves problems of external coordination revealed by command and staff visits and information gathering. During internal coordination, the G-7 resolves problems and conflicts. It also ensures that resources allocated to support units assigned IO tasks actually arrive. The G-7 uses the IO execution matrix as an assessment tool. It displays information that supports monitoring and evaluating coordination. Examples of internal coordination include—

- Deconflicting PSYOP and public affairs (PA) products.
- Monitoring the progress of answers to IO IRs.
- Monitoring RFIs to higher headquarters by the G-3 current operations, with notification to the G-7.
- Checking the air tasking order for missions requested by the G-7.
- Monitoring the movements and readiness of IO assets.
- Determining space asset status and space weather implications.
- Participating in the integration of IO-related targets into the targeting process.
- Using figure 2-1 (pages 2-27–2-30) to coordinate IO elements that support each other.
- Using figure 2-2 (pages 2-31–2-32) to deconflict those elements that conflict with each other.
- Using figure 2-3 (page 2-33) to see how the elements of IO support or conflict with the related activities of PA and CMO (all IO cell members; see appendix F).
- Continuous monitoring and validation of OPSEC procedures, particularly in preparation for military deception. This could include a short statement on physical security, particularly during movement.

6-42. The G-7 remains mindful that training is conducted during planning and preparation. This occurs particularly as new soldiers and IO capabilities are integrated into the command and the command's battle rhythm.

6-43. Each staff officer has responsibilities during preparation for each of the IO elements. Examples related to some IO elements follow:

- **Electronic warfare.**
  - G-1—Identify personnel with cryptologic and linguistic skills to support EW operations.
  - G-2—Coordinate intelligence gathering in support of the EW mission. Recommend the use of EW against adversary surveillance measures.
  - G-3—Coordinate the priority targets for electronic countermeasures.
  - G-4—Coordinate distribution of EW equipment and supplies, less cryptographic support.
  - G-5—Coordinate for use of host-nation personnel with special linguistic qualifications.
  - EW officer—Monitor the preparation of military intelligence units with EW missions.

- **Psychological operations.**
  - G-1—Assist in the administration and control of civilian personnel who have skills desired by PSYOP units.
  - G-2—Prepare intelligence estimate and analysis of the area of operation.
  - G-3—Request additional PSYOP units as required.
  - G-4—Prepare logistic support of PSYOP.
  - G-7—Identify requirements for additional PSYOP units to the G-3.
  - PSYOP officer—Prepare the PSYOP appendix to IO annex. Prepare the PSYOP estimate.
- **Operations security.**
  - G-1—Procure, when required, civilian resources for use as guard forces.
  - G-2—Provide data on adversary intelligence.
  - G-4—Advise on the vulnerabilities of supply, transport, and maintenance facilities, and lines of communications.
  - G-5—Determine availability of civilian resources for use as guard forces.
  - G-7—Determine the EEFI.
  - OPSEC officer—Prepare the OPSEC estimate and appendix.
  - Provost marshal—Advise on physical security measures.
- **Military deception.**
  - G-1—Coordinate personnel support requirements to implement the MD plan.
  - G-2—Determine adversary surveillance capabilities.
  - G-3—Coordinate movement of units participating in MD.
  - G-4—Coordinate logistic support to carry out assigned deception tasks.
  - G-5—Coordinate host-nation support to implement the MD plan.
  - MD officer—Prepare to monitor execution of MD operation.

EXTERNAL COORDINATION

6-44. External coordination includes coordinating with or among subordinate units and higher headquarters. This coordination concerns IO assets and resources or forces that may not be under the unit's control during planning. These IO assets may be available during preparing or executing. External coordination also includes coordinating with adjacent units or agencies. (In the information environment, adjacent refers to any organization that can affect a unit's operations.) This coordination is necessary to synchronize IO throughout the force. Examples of external coordination include—

- Ensuring preparation of PSYOP and PA products, including release approval.
- Assessing unit OPSEC posture.
- Making sure the MD operation is tracking with preparation for the overall operation.
- Periodically validating assumptions.

- Ensuring MD operations are synchronized with those of higher, lower, and adjacent units.
- When possible, the G-7 requires each unit, detachment, and section involved in IO to backbrief its responsibilities. This ensures a comprehensive understanding of their tasks and how each task is synchronized within the IO concept of support.

6-45. The G-7 remains aware of the effectiveness of computer network defense actions/tasks, including information assurance tasks taken by the G-6. Proper protection of plans and orders, and refinements to them, is essential during operations.

LIAISON

6-46. Establishing and maintaining liaison is one of the most important means of external coordination (see FM 6-0). The G-7 may perform liaison through the command's liaison officers; a member of the G-7 may be part of a liaison team. Establishing liaison early in planning supports effective coordination.

6-47. Practical liaison can be achieved through personal contact between G-7s. This is accomplished through the exchange of liaison personnel, through agreement on mutual support between adjacent units, or through a combination of these means. Liaison should, when possible, be reciprocal between higher, lower, and adjacent units. Liaison must be reciprocal between IO sections when US forces are operating with or adjacent to, multinational partners.

6-48. Liaison also has a force protection mission. Where host-nation security forces retain some operational capability, liaison is vital to coordinate actions. In some cases, it may be more important to coordinate with host-nation security forces than with Army forces. In nearly all cases, they provide intelligence and other related information about conditions in-theater.

REHEARSALS

6-49. The G-7 participates in unit rehearsals to ensure IO is synchronized with the overall operation and to identify potential problems during execution. The G-7 may conduct further rehearsals of IO tasks and actions to ensure coordination and synchronization of IO among units assigned them. Before participating in a rehearsal, the G-7 reviews the plans or orders of subordinate and supporting commands (see paragraph 6-8).

6-50. Commanders and staffs use a form of rehearsal called a rock drill. A rock drill is a leader and staff rehearsal that usually uses a sand table or similar training aid. Its primary purpose is to synchronize the actions of all battlefield operating systems. IO are fully integrated into rock drills and other staff rehearsals. Doing this ensures all concerned know their IO tasks and understand how IO may affect their functional responsibilities. Rehearsals also verify the timing of IO execution relative to the overall operation.

TASK ORGANIZATION AND MOVEMENTS

6-51. The G-7 coordinates with the G-3 for movement of IO assets and resources during preparation. The G-7 integrates movements of units assigned IO tasks with OPSEC measures to ensure that they do not reveal any intentions. IO-capable units involved in MD operations adhere strictly to the MD plan so as not to compromise it. This is a carryover from planning.

6-52. Units cannot be assigned missions supporting IO objectives and given IO tasks without first receiving the capabilities needed to execute them. For example, a divisional maneuver brigade does not have an S-7 section. It requires augmentation if it is detached and assigned a mission involving IO. One procedure to overcome the lack of an organic S-7 is to attach a staff officer from the G-7 section to the brigade headquarters to synchronize IO elements.

PREOPERATION CHECKS AND INSPECTIONS

6-53. As with other units, units assigned IO tasks complete preoperation checks and inspections. The G-7 role is staff coordination, which ensures that resources are provided according to by the commander's priorities. Preparation includes checks and inspections of soldier training and systems used to execute the mission. All IO systems are checked without revealing these checks to the adversary.

LOGISTIC PREPARATIONS

6-54. Resupplying, maintaining, and issuing special supplies or equipment to or in IO-capable units takes place during preparation. Repositioning of logistic assets for units assigned IO tasks also occurs during preparation. The G-7 coordinates with the G-4 to ensure that units assigned IO tasks receive the necessary support. The G-7 ensures that these preparations do not violate OPSEC measures.

INTEGRATION OF NEW SOLDIERS AND IO-CAPABLE UNITS

6-55. The G-7 assures that IO-capable units made available to the force are fully integrated into the command in a posture that allows them to contribute effectively. This responsibility includes integrating any support received from the 1st Information Operations Command (Land). The G-7 ensures that IO-capable units are prepared to perform their IO tasks.

SUMMARY

6-56. Preparation begins during planning and continues through execution. IO preparation raises the readiness of units assigned IO tasks. It includes, but is not limited to, plan or order refinement, force protection, coordination and liaison, rehearsals (unit and IO-specific), task organization, and adjustment and movement of IO-capable units. Preparation combines preoperation checks and inspections of IO assets, logistic preparations, and integration of new soldiers and IO-capable units into the force's mission until committed by the commander. It also involves reviewing plans and orders of

subordinate and supporting units to identify conflicts and to ensure IO synchronization. Rehearsals offer the G-7 opportunities to identify and resolve IO issues before execution. Preparation for IO often requires longer lead times than preparation for other types of operations.

Chapter 7

Executing Information Operations

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

STAFF COORDINATION

7-1. The challenges faced by the G-7 are how to assess IO execution and how to adjust IO as the operation unfolds. Simultaneously, the G-7 integrates the IO elements. The G-7 assists the G-3 in synchronizing IO with the overall operation.

7-2. IO execution is critically dependent on the intelligence battlefield operating system for three reasons. First, intelligence provides an assessment of IO effects on adversaries and others, and of their reactions to counter these effects. Second, intelligence provides a real-time assessment of how adversaries and others are attempting to degrade friendly C2. Third, intelligence operates many of the Army's airborne and ground-based sensors and jammers that play a vital role in both offensive and defensive IO. It also converts the information they collect into intelligence.

CONTENTS

7-3. The requirement for responsive staff coordination among the IO elements intensifies during execution as an operation progresses and variances from the operation order (OPORD) increase. The decentralized nature of IO execution, combined with the multiple command levels involved and the allocation of information monitoring responsibilities among the unit's command posts (CPs), place a heavy demand on the G-7.

7-4. A headquarters monitors the effects of its own IO and coordinates any activities that may directly affect the operations of other commands. To do this, the G-7 establishes links with higher and adjacent command G-7s to obtain effects assessments in near real-time. With this information, the G-7 tracks how the effects of other organizations' IO impact the command's overall operation.

7-5. IO execution is complicated because the tactical command post (TAC CP), main CP, and rear CP each monitor different parts of the operation. Continuous exchange of information among the G-7s, S-7s, and others responsible for controlling IO at these CPs is paramount.

7-6. The TAC CP directs IO execution and adjusts missions as required. The IO cell in the TAC CP provides initial assessment of IO effectiveness. It—

- Maintains the IO portion of the common operational picture (COP) to support current operations.
- Maintains a picture of the adversary C2 system.
- Maintains IO information requirement (IR) status.
- Coordinates preparation and execution of IO with maneuver and fires.
- Recommends adjustments to current IO.
- Tracks IO assets and recommends repositioning of IO assets as required.
- Tracks IO-related targets in conjunction with the G-2.
- Nominates targets for attack.

7-7. The main CP plans, coordinates, and integrates IO. It—

- Creates and maintains IO aspects of the COP.
- Maintains the IO estimate.
- Incorporates answers to IO IRs into the IO estimate.
- Maintains a current IO order of battle.
- Deconflicts IO internally and externally.
- Requests/coordinates IO support with other battlefield operating system representatives, outside agencies, higher headquarters, and augmenting forces.
- Identifies future IO objectives based on successes or failures of current operations.

7-8. The rear CP answers IO IRs that the main and TAC CPs cannot answer. When necessary, it obtains augmentation to meet special needs or shortfalls. In addition, IO representatives at the rear CP—

- Advise rear CP staff on IO.
- Coordinate IO support with outside agencies, higher headquarters, and augmenting IO forces.

- Integrate out-of-theater and national information sources into the targeting process.

7-9. The G-7 receives reports from elements executing IO tasks and keeps the chief of staff (COS) informed on IO status. Changes in taskings are planned and coordinated by the G-7 and disseminated by fragmentary orders (FRAGO) from the G-3 (see appendix G.)

ASSESSING INFORMATION OPERATIONS DURING EXECUTION

7-10. *Assessment* is the continuous monitoring—throughout planning, preparation, and execution—of the current situation and progress of an operation, and the evaluation of it against criteria of success to make decisions and adjustments (FM 3-0).

7-11. The G-7 compiles information from all CPs, the G-2, and higher headquarters to maintain a continuous IO assessment in the IO estimate (see appendix C). The primary objective of assessment is to determine whether IO are having the desired effects. As the situation changes, the G-7 and G-3 make sure IO remains fully synchronized with the overall operation.

7-12. IO assessments are derived from monitoring IO task execution. IO assessments evaluate the effects of friendly offensive IO and defensive IO. Offensive IO are evaluated in terms of their effects on adversary C2 systems and the information environment. Defensive IO are evaluated in terms of how well they counter adversary IO. Assessment allows the G-7 to decide either to recommend continuing IO as specified by the OPORD, or to alter the plan (usually with a FRAGO) to fit the situation.

7-13. IO assessment begins during planning. At that time, the commander and staff determine the IO tasks to be assessed, the criteria of success, and the means of obtaining the required information. During orders production, the G-7 planner uses this information to prepare the IO assessment matrix. (See figure B-26, pages B-39–B-42). During execution, the G-7 uses the execution matrix to control IO execution and the assessment matrix to determine when and where to obtain information to assess IO tasks. The measures of performance in FM 7-15 may be used as the basis for criteria of success for IO tasks.

MONITORING INFORMATION OPERATIONS

7-14. The G-7 monitors IO to determine progress towards achieving the IO objectives. Once execution begins, the G-7 monitors the adversary and friendly situations to track IO task accomplishment, determine the effects of IO during each phase of the operation, and detect and track any unintended consequences of the IO.

7-15. Monitoring the execution of defensive IO is done at the main CP because it is the focal point for intelligence analysis and production, and because the command's C2 nodes are monitored there. The G-7 works closely with G-2 and IO cell representatives to provide a running assessment of the effectiveness of adversary IO and keeps the COS informed. The main CP is where offensive and defensive IO are collectively reviewed and where the IO effectiveness is assessed.

7-16. With G-2, G-3, and fire support representatives, the G-7 monitors offensive IO execution in the TAC CP and the main CP. The G-7 is concerned with attacking adversary C2 nodes with airborne and ground-based jammers, fire support, attack helicopters, and tactical air. After preplanned IO-related high-payoff targets (HPTs) have been struck, the strike effectiveness is assessed. Effective IO support of current operations depends on how rapidly the TAC CP can perform the targeting cycle to strike targets of opportunity. The IO representative in the TAC CP monitors the effectiveness of friendly communications and recommends actions to maintain or improve communications nodes and links. The G-3 representative in the TAC CP keeps the main CP informed of current operations, including IO.

7-17. Monitoring IO execution at the rear CP focuses principally on maintaining freedom of movement and uninterrupted operations in the rear area. From an IO perspective, the rear CP focuses on forces and organizations that could disrupt the C2 of sustaining operations and the flow of assets into the forward areas. Most rear CP attention is concentrated on reducing terrorist or special operations force threats, sustaining civil infrastructure, and supporting the deployed force. Normally, the support command's operations and intelligence staffs monitor and direct IO in the rear area, reporting plans and activities to the main CP.

7-18. To organize and portray IO execution, the G-7 uses various staff devices and aids. Some useful aids are—

- **IO execution matrix**. Either the execution matrix taken directly from the IO annex, or an extract containing only the current and near-term IO tasks, may be used, depending on the complexity of the operation. The execution matrix is used by the G-7 to monitor progress and results of IO objectives and tasks, and to keep IO execution focused on contributing to the overall operation (see figure D-6, page D-15; figure D-8, page D-20).
- **Decision support template**. The decision support template produced by the G-3 is used by the G-7 to monitor progress of IO in relation to decision points and any branches or sequels.
- **High-payoff target list**. The G-7 maintains a list or graphic (for example, a link and node diagram) to track the status of IO-related HPTs identified during planning.
- **Critical assets list**. The G-7 uses the critical assets list to monitor the status of critical friendly information nodes and the status of critical systems supporting IO, for example, electronic warfare systems, psychological operations (PSYOP) assets, and deep attack assets.

EVALUATING INFORMATION OPERATIONS

7-19. During execution, the G-7 works with the G-2, G-3, and the analysis and control element (ACE) to obtain the information needed to determine the individual and collective IO effects.

7-20. Evaluation not only estimates the effectiveness of task execution, but also evaluates the effect of the entire IO effort on adversaries, other key people in the area of operations (AO), and friendly operations. One way to evaluate the IO contribution to the overall operation is to compare IO progress

against the IO objectives. This can be done by confirming execution of IO tasks and monitoring reports on adversary reactions to judge each task's effects. An analysis of these individual effects may help determine the total effect of all the IO tasks on adversary operations. It allows an assessment of whether the adversary is acting as envisioned during planning. The G-7 may use an IO assessment matrix to capture and record assessment information (see figure B-26, pages B-39–B-42).

7-21. Based on the IO effects evaluation, the G-7 adjusts IO to further exploit adversary vulnerabilities, redirects actions yielding few effects, or terminates actions after they have achieved the desired result. The G-7 keeps the COS and commander informed of IO effects and how these impact friendly and adversary operations. Some of the possible changes to IO are—

- Strike a target or continue to protect a critical asset to ensure the desired effect.
- Execute a branch or sequel.

DECISIONMAKING DURING EXECUTION

7-22. Decisionmaking during execution includes—

- Executing IO as planned.
- Adjusting IO to a changing friendly situation.
- Adjusting IO to an unexpected adversary reaction.

EXECUTING INFORMATION OPERATIONS AS PLANNED

7-23. Essential to execution is a continuous information flow among the G-2, G-3, G-7, and ACE (see figure 7-1, page 7-6). The G-7 tracks execution with the G-3 and ACE. The IO targeting officer coordinates with the targeting staff for feedback on IO tasks and IO-related targets.

7-24. To execute IO, the G-7 maintains an execution matrix. This matrix is periodically updated and provided to the G-2, G-3, and ACE. Using the matrix, the G-7 keeps a record of completed IO tasks. As tasks are completed, the G-7 passes the information to the ACE. The G-7 uses this information to keep IO synchronized with the overall operation.

7-25. The G-7 determines whether the adversary commander and other targeted leaders are reacting to IO as anticipated during course of action (COA) analysis. The G-7 also looks for new adversary vulnerabilities and for new IO-related targets. The G-7 proposes changes to the OPORD to deal with variances throughout execution. The G-3 issues FRAGOs pertaining to IO as requested by the G-7. These FRAGOs may implement changes to the IO concept of support, IO objectives, and IO tasks. The G-7 updates the IO execution matrix and IO assessment matrix to reflect these changes.

7-26. Given the flexibility of advanced information systems, the time available to exploit new adversary C2 vulnerabilities may be limited and require an immediate response from several IO elements. Actions to defeat adversary IO need to be countered immediately. The G-3 may issue a verbal FRAGO when immediate action is required.

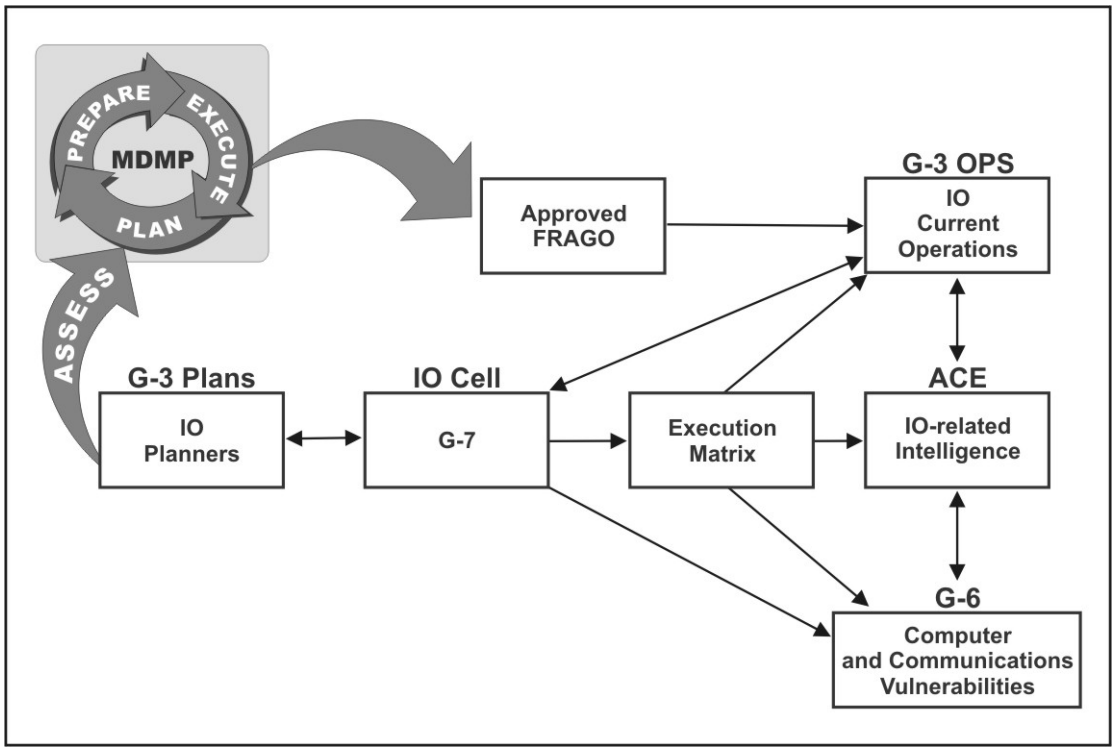


Figure 7-1. Information Operations Execution at the Main Command Post

ADJUSTING INFORMATION OPERATIONS TO A CHANGING FRIENDLY SITUATION

7-27. IO will not be executed exactly as planned. Possible reasons for a variance from the plan include—

- An IO task is aborted or assets redirected.
- An IO-related target did not respond as anticipated.
- The adversary effectively countered an IO attack.
- The adversary successfully disrupted friendly C2.
- The initial plan did not identify an IO-related target/target of opportunity.

7-28. The G-7's challenge under these circumstances is to rapidly assess how changes in IO execution affect the overall operation and to determine necessary follow-on actions. Based on the commander's input, the G-7—in coordination with the G-2, G-3, and ACE—considers COAs, conducts a quick COA analysis, and determines the most feasible COA.

7-29. If the selected COA falls within the decisionmaking authority of the G-3, IO execution can be adjusted without notifying the commander. When changes exceed previously designated limits, the G-7 obtains approval from the commander. At this point, a more formal decisionmaking process may be required before issuing a FRAGO, especially if a major adjustment to the operation order (OPORD) is needed. In such a case, the G-7, working with the G-3, participates in a time-constrained military decisionmaking process to develop a new COA.

ADJUSTING INFORMATION OPERATIONS TO AN UNEXPECTED ADVERSARY REACTION

7-30. Adversaries may react in an unexpected manner to IO or to the overall operation. If adversary actions diverge significantly from those anticipated when the OPORD was written, the commander and staff look first at branch and sequel plans. If branch or sequel plans fail to adequately address the new situation, a new planning effort may be required.

7-31. The G-7 prepares branches that modify and direct defensive IO when adversary actions cause new friendly C2 vulnerabilities, or when friendly offensive IO prove ineffective. The G-3 and ACE work with the G-7 to maintain a running assessment of adversary capability to disrupt friendly C2, and look for ways to lessen friendly vulnerabilities. Concurrently, they look for opportunities to reestablish offensive IO effectiveness. Under these conditions, the G-7 determines the adequacy of existing branches and sequels. If none fit the situation, they create a new branch or sequel and disseminate it by FRAGO.

7-32. If a new plan is needed, time available dictates the length of the decision-making process and the amount of detail contained in an order. The G-7 may only be able to use IO elements that can immediately affect the overall operation: for example, physical destruction, electronic warfare, and sometimes PSYOP. Other IO elements proceed as originally planned and are adjusted later, unless they conflict with the new plan.

OTHER CONSIDERATIONS

7-33. Other considerations include, but are not limited to—

- IO exection begins early.
- IO delivers unanticipated results.

INFORMATION OPERATIONS EXECUTION BEGINS EARLY

7-34. A potential adversary commander begins forming a perception of a situation well before encounters with friendly forces. Recognizing this fact, commanders establish a baseline of IO that is practiced routinely in garrison and training. Selected IO elements (for example, PSYOP, operations security (OPSEC), military deception, and public affairs) may begin contributing to an IO objective well before a deployment occurs. To support early execution of the overall operation, IO planning, preparation, and execution frequently begins well before the staff starts planning for an operation.

INFORMATION OPERATIONS DELIVERS UNANTICIPATED RESULTS

7-35. It is difficult to estimate how offensive and defensive IO will affect an operation. Actions by decisionmakers, the ultimate target of IO, sometimes take surprising turns, uncovering unanticipated weaknesses or strengths. Similarly, friendly commanders, stressed by attacks on their C2 system, may react unexpectedly. Flexibility is key to success in IO execution. Effective commanders and well-trained staffs are flexible enough to compensate for adversary IO, while exploiting both projected and unanticipated adversary vulnerabilities.

SUMMARY

7-36. Successful IO execution relies on teamwork by several staff sections and rapid information exchange among them. As an operation unfolds and the situation becomes increasingly fluid, IO objectives and tasks are modified to exploit success and protect friendly vulnerabilities. The G-7 prepares branches and sequels to allow the commander to rapidly adjust IO when necessary. The G-7 also prepares to coordinate changes with other staffs and headquarters.

Appendix A

Quick Reference to IO Input to the MDMP

This appendix lists the IO planning actions and IO products associated with each task and subtask of the military decisionmaking process. It includes the sources of information needed for each task. Refer to chapter 5 for details. Refer to appendix B for a scenario and examples of corps-level IO products. Refer to appendix C for an example of an IO estimate. Refer to appendix D for an example of an IO annex.

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
Receipt of Mission	• Higher HQ OPLAN/ OPORD or deduced mission (figure B-2, page B-3) • Commander's initial guidance (figure B-3, page B-5) • IO estimate (appendix C)	• Participate in commander's initial assessment • Receive the commander's initial guidance (figure B-3, page B-5) • Perform an initial IO assessment • Prepare for subsequent planning • Allocate time to perform tasks	• Input to initial IPB, including initial EEFI (OPSEC) • Input to initial ISR tasking (IO IRs); include IO IRs concerning adversary capability to collect EEFI (OPSEC) • Submit IO IRs concerning adversary capability to collect EEFI to G-2 (OPSEC) • IO input to first WARNO; input includes initial EEFI (figure B-4, page B-6) • Recommend initial EEFI to G-2 & G-3 (OPSEC) • Assemble DWG; begin MD mission analysis (MD) • Update IO estimate • Allocate available time

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
Mission Analysis— Analyze the Higher HQ Order	• Higher HQ OPLAN/OPORD, particularly the IO annex • Commander's intent two echelons up • Commander's initial IO guidance	• Understand higher commander's intent and concept of operations • Understand higher commander's AO, mission-task constraints, acceptable risk, available assets • Understand higher commander's schedule for conducting operations • Understand missions of adjacent units • Analyze the mission from an IO perspective • Determine IO-related tasks assigned to the unit by higher HQ • Identify information needed for IO planning	• IO-related tasks assigned to the unit by higher HQ
Mission Analysis— Conduct IPB	• Higher HQ IPB • Higher HQ staff estimates • Higher HQ OPLAN/OPORD	• Develop IO input to the IPB • Analyze key friendly and adversary leaders and decisionmakers, supporting decisionmaking processes, INFOSYS, and C2 systems • Identify adversary IO-related capabilities and vulnerabilities • Analyze friendly IO capabilities and vulnerabilities • Identify gaps in current intelligence on adversary IO • Derive IO-related HPTs • Describe the part of the information environment in the commander's battlespace and its effect on friendly and adversary IO • Determine probable IO COAs • Assess the potential effects of IO on adversary operations • Determine additional EEFI (OPSEC)	• Provide IO input to IPB products. These become part of paragraph 2 of the IO estimate (figure B-5, page B-9) • Submit IO IRs to G-2 • Nominations to HPTL for lethal and nonlethal attack (targeting) • Refined EEFI (OPSEC)

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
Mission Analysis— Determine Specified, Implied, and Essential Tasks	• Specified and implied IO-related tasks from higher HQ OPLAN/OPORD • IPB products	• Identify specified and implied IO-related tasks in the higher HQ OPLAN/OPORD. • Develop IO-related implied tasks • Determine additional EEFI (OPSEC) • Develop IO input to the command targeting guidance • Assemble critical asset list	• IO-related tasks (figure B-6, page B-11) • Refined EEFI (OPSEC) • Provide critical asset list to G-3 (figure B-6, page B-11) • IO input to the command targeting guidance
Mission Analysis— Review Available Assets	• Current task organization (for IO assets) • Higher HQ task organization (for IO resources) • Status reports • Unit SOP	• Identify friendly IO assets and resources • Determine if available assets can perform all IO-related tasks • Identify additional resources (such as fire support assets) needed to execute or support IO • Compare available assets and resources to IO-related tasks	• List of available IO assets and capabilities (IO estimate paragraph 2c) (figure B-7, page B-12) • Requests for additional IO resources, if necessary
Mission Analysis— Determine Constraints	• Commander's initial guidance • Higher HQ OPLAN/OPORD	• Identify constraints (requirements and prohibitions) on IO, including those that affect possible OPSEC measures	• List of constraints on IO, including those that affect possible OPSEC measures (IO annex concept of support or coordinating instructions) (figure B-8, page B-13)
Mission Analysis— Identify Critical Facts and Assumptions	• Higher HQ OPLAN/OPORD • Commander's initial guidance • Observations and reports	• Identify facts and assumptions affecting IO elements • Submit IO IRs for information that will confirm or disprove facts and assumptions • Identify facts and assumptions that regarding OPSEC indicators that result in OPSEC vulnerabilities	• List of facts and assumptions pertinent to IO elements (IO estimate paragraph 2) (figure B-9, page B-13) • IO IRs for information that will confirm or disprove facts and assumptions
Mission Analysis— Conduct Risk Assessment	• Higher HQ OPLAN/OPORD • IPB • Commander's initial guidance	• Identify and assess hazards associated with IO • Identify OPSEC indicators • Assess risk associated with OPSEC indicators to determine OPSEC vulnerabilities • Establish provisional OPSEC measures	• List of assessed hazards to IO • IO input to risk assessment (figure B-10, page B-14) • List of provisional OPSEC measures

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
Mission Analysis— Determine Initial CCIR	• IO IRs	• Determine information the commander needs to make critical IO decisions or to assess IO actions • Identify IO IRs to recommend as CCIR	• IO IRs nominated as CCIR (figure B-12, page B-16)
Mission Analysis— Prepare the initial ISR Annex	• Initial IPB • PIRs/IO IRs	• Identify gaps in information needed to support IO planning and execution and assessment of early-initiation actions • Confirm that the initial ISR annex includes IO IRs concerning adversary capability to collect EEFI	• IO IRs for information needed to support IO planning and execution and assessment of early-initiation actions • IO IRs concerning adversary capability to collect EEFI
Mission Analysis— Plan Use of Available Time	• Revised G-3 time plan	• Determine time required to accomplish IO objectives • Compare time available to accomplish essential IO-related tasks within the higher HQ time line and the adversary time line developed during IPB • Refine initial time allocation plan	• IO time line (provided to G-3), with emphasis on the effect on IO of long lead-time events
Mission Analysis— Write the Restated Mission	• Initial IO mission • Initial IO objectives	• Recommend possible IO objectives for inclusion in the restated mission	• IO-related essential tasks • Restated IO mission • IO objectives recommended for inclusion in the restated mission
Mission Analysis— Conduct Mission Analysis Briefing	• IO estimate • Unit SOP	• Prepare to brief IO portion of mission analysis • Brief MD estimate	• IO portion of mission analysis briefing (figure 5-4, page 5-18) • MD estimate
Mission Analysis— Approve the Restated Mission	• Restated mission • Mission analysis briefing	• Receive and understand the approved mission statement	• None
Mission Analysis— Develop Initial Commander's Intent	• Higher HQ commander's intent • Results of mission analysis • IO estimate	• Develop recommended IO input to the commander's intent	• Recommend IO input to the commander's intent (figure B-14, page B-17)

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
Mission Analysis— Issue Commander's Guidance	• Higher HQ OPLAN/OPORD • Results of mission analysis • IO estimate	• Develop recommended IO input to the commander's guidance • Combine the refined EEFI with the provisional OPSEC measures to produce the OPSEC planning guidance	• Recommended IO input to the commander's guidance (figure B-15, page B-17) • Recommended OPSEC planning guidance • Recommended MD guidance • Recommended IO targeting guidance
Mission Analysis— Issue Warning Order	• Commander's guidance and intent • Approved restated mission, restated IO mission, and initial IO objectives • IO mission analysis products	• Prepare input to the warning order. Input may include— ▪ Develop early taskings to subordinate units ▪ Initial IO mission statement ▪ OPSEC planning guidance ▪ Reconnaissance and surveillance taskings ▪ MD guidance	• Input to mission, commander's intent CCIR, and concept of operations (see figure B-16, page B-18) • Recommend the initial IO mission statement
Mission Analysis— Review Facts and Assumptions	• Commander's guidance and intent • Approved restated mission • IO mission analysis products	• Review IO facts and assumptions • Refine initial IO mission statement	• Updated facts and assumptions • Refined IO mission statement • Refined OPSEC measures
COA Development— Analyze Relative Combat Power	• IPB • Task organization • IO estimate • Vulnerability assessment	• Analyze IO effects on friendly and adversary capabilities, vulnerabilities, and combat power	• Description of the potential effect of IO on the relative combat power, stated by IO element
COA Development— Generate Options	• Commander's guidance and intent • IPB • Adversary and friendly IO assets, resources, and vulnerabilities	• Develop different ways for IO to support each COA • Determine IO elements to use • Determine how to focus IO on the overall objective • Determine IO's role in the decisive and shaping operations of each COA • Determine possible tradeoffs between IO and other assets • Develop MD COAs (deception stories)	• IO concept of support for each COA • One or more MD COAs

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
COA Development— Array Initial Forces	• Restated mission • Commander's intent and guidance • IPB • MD plan or concept	• Allocate assets for each IO concept of support • Identify requirements for additional IO resources • Examine effect of possible MD COAs on force positioning • Identify MD means	• Initial IO asset locations • Additional IO resource requirements
COA Development— Develop Concept of Operations	• COAs (figure B-17, page B-22) • IPB • HVTL • IO mission statement • Initial IO concept of support for each COA	• **For each COA—** • Develop IO concept of support (figures B-18, page B-24) • Develop IO objectives • Synchronize IO element actions • Identify and prioritize offensive and defensive IO tasks • Nominate selected HVTs as HPTs • Determine initial IO task execution time line • Refine IO input to risk assessment • Develop IO assessment plan • Identify additional EEFI • Identify and assess OPSEC indicators to determine OPSEC vulnerabilities • Develop OPSEC measures to shield OPSEC vulnerabilities • Determine residual risk associated with each OPSEC vulnerability after OPSEC measures are applied (figure B-24, page B-34) • Determine feedback required for assessment of MD COAs • Conduct a risk assessment for each MD COA • Conduct an OPSEC analysis for each MD COA • Prepare termination branches for each MD COA	• **For each COA—** • IO input work sheet containing a refined IO concept of support, IO objectives, and IO tasks (figures B-19 through B-22, pages B-19–32) • IO execution time line • IO-related HPT nominations • Critical asset list • IO input to risk management plan, including residual risk associated with each OPSEC vulnerability (figure B-24, page B-34) • Criteria of success and IO IRs to support IO assessment • Additional EEFI • OPSEC vulnerabilities • OPSEC measures (IO tasks) to shield OPSEC vulnerabilities

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
COA Development— Recommend Headquarters	• IPB • IO estimate • IO vulnerability assessment • IO tasks by IO element	• Assess C2 strengths and weaknesses to determine IO-related vulnerabilities of specific HQ • Reevaluate critical asset list	• Recommendations concerning role of HQ in light of C2 vulnerability assessment • Updated critical asset list • Initial list of assets/re–sources to tasks assigned
COA Development— Prepare COA Statements and Sketches	• COA statement • An IO concept of support and IO objectives for each COA	• Submit input for each COA statement/sketch to G-3 • Prepare IO concept of support statement and sketch for each COA	• Input for each COA statement/sketch • IO concept of support sketches for each COA, stating the most important IO objectives
COA Analysis	• COAs • IPB • IO input worksheets • IO execution time line	• Develop evaluation criteria for each COA • Synchronize IO tasks performed by different IO elements • Integrate IO concept of support into the concept of operations for each COA • Synchronize IO concept of support with that of higher and adjacent HQ • Identify adversary IO capabilities and likely actions and reactions • War-game friendly IO capabilities against adversary vulnerabilities • War-game adversary IO capabilities against friendly vulnerabilities • Synchronize and deconflict initial IO tasks • Refine targeting guidance and HPTL • Synchronize and deconflict IO targets • Determine whether modifications to the COA result in additional EEFI or OPSEC vulnerabilities; if so, recommend OPSEC measures to shield them • Assign attack measures to HPTs	• An evaluation of each MD COA in terms of criteria established before the war game **For each COA—** • An evaluation in terms of criteria established before the war game • Refined IO input worksheets • Refined IO concept of support • Refined IO objectives • Refined IO tasks • Refined IO input to AGM and TSM • IO IRs and RFIs identified during the war game • Refined EEFI and OPSEC vulnerabilities, and OPSEC measures • Paragraph 3 of the IO estimate • IO input to G-3 synchronization matrix • IO input to HPTL

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
		• Test OPSEC measures • Determine decision points for executing OPSEC measures • Determine operational support needed for OPSEC measures • Determine OPSEC measures needed to support possible OPSEC branches and sequels • Determine whether any OPSEC measures require addition coordination • War-game each MD COA • Identify each MD COA's potential branches; assess risk to the COA • List the most dangerous/beneficial branch on IO decision support template or IO execution matrix	
COA Comparison	• COA evaluations from COA analysis • COA evaluation criteria	• Compare the COAs with each other to determine the advantages and disadvantages of each • Determine which COA is most supportable from an IO perspective • Determine if any OPSEC measures require the commander's approval	• IO advantages and disadvantages for each COA • Determine which COA is most supportable from an IO perspective • IO COA decision matrix • Paragraph 4, IO estimate

MDMP Task	Information Sources (Inputs)	G-7 Actions	G-7 Products
COA Approval	• Results from COA comparison • Recommended COA	• Provide IO input to COA recommendation • Reevaluate IO input to the commander's guidance and intent • Refine IO concept of support, IO objectives, and IO tasks for approved COA and develop associated IO execution matrix • Prepare IO input to the WARNO • Participate in COA decision briefing • Recommend COA that IO can best support • Request decision on executing any OPSEC measures that entail significant resource expenditure or risk	• Finalized IO concept of support for approved COA • Finalized IO objectives and IO tasks based on approved COA • IO input to WARNO (figure B-25, page B-36) • IO execution matrix
Orders Production	• Approved COA • Refined commander's guidance • Refined commander's intent • IO estimate • IO execution matrix • Finalized IO mission statement, IO concept of support, IO objectives, and IO tasks	• Ensures IO input (such as, EEFI and IO tasks to subordinate units) is placed in base OPLAN/OPORD • Finalize IO annex • Coordinate IO objectives and tasks (including OPSEC measures) with IO element staff officers • Conduct other staff coordination • Refine IO execution matrix	• IO synchronization matrix • IO subparagraph to base OPLAN/ OPORD • IO annex • IO input to the AGM and TSM • MD appendix to IO annex

Appendix B

Information Operations Scenario

This appendix contains sample corps-level information operations (IO) products based on a notional scenario. The products and tasks it outlines apply during war and military operations other than war. The products are illustrated in the order they are developed during the military decisionmaking process (MDMP). (Appendix A lists G-7 actions and products associated with each MDMP task. Appendix D includes an example IO annex based on this scenario. Appendix G includes an example of an IO-focused fragmentary order based on this scenario.) The products illustrated are examples only and are not intended to be authoritative or prescriptive. They contain the minimum information needed to show how to develop an IO concept of support. They are not intended to be complete.

General Scenario

Six months ago, the nation of Rendova invaded its smaller neighbor, the Republic of San Anglos (see figure B-1, page B-2). Both San Anglos and Rendova have had ties to the United States since the Spanish-American War. San Anglos is an island approximately 300 kilometers east to west and 200 kilometers north to south. The Strait of Dawaro, which is 45 kilometers wide, separates it from Rendova, The western half of San Anglos has a significant ethnic Rendovan minority. Most work as laborers, although some are middle class. Rendova used alleged exploitation of this minority to justify its invasion and has drawn significant support from it.

The stated Rendovan war aim is to "liberate" the ethnic Rendovans in western San Anglos. However, Rendovan actions make it appear that they intend to conquer the entire island. The Army of San Anglos (ASA) was able to stop the Rendovan advance and stabilize the front after two months of fighting. Rendovan forces occupy the western

CONTENTS

third of San Anglos. The ASA controls the rest. Rendova is now talking in terms of partitioning San Anglos and annexing the territory it now holds. The Government of San Anglos does not consider partition acceptable. It believes it can expel the Rendovan invaders. However, the Government believes that the longer Rendovan forces remain, the harder it will be to expel them.

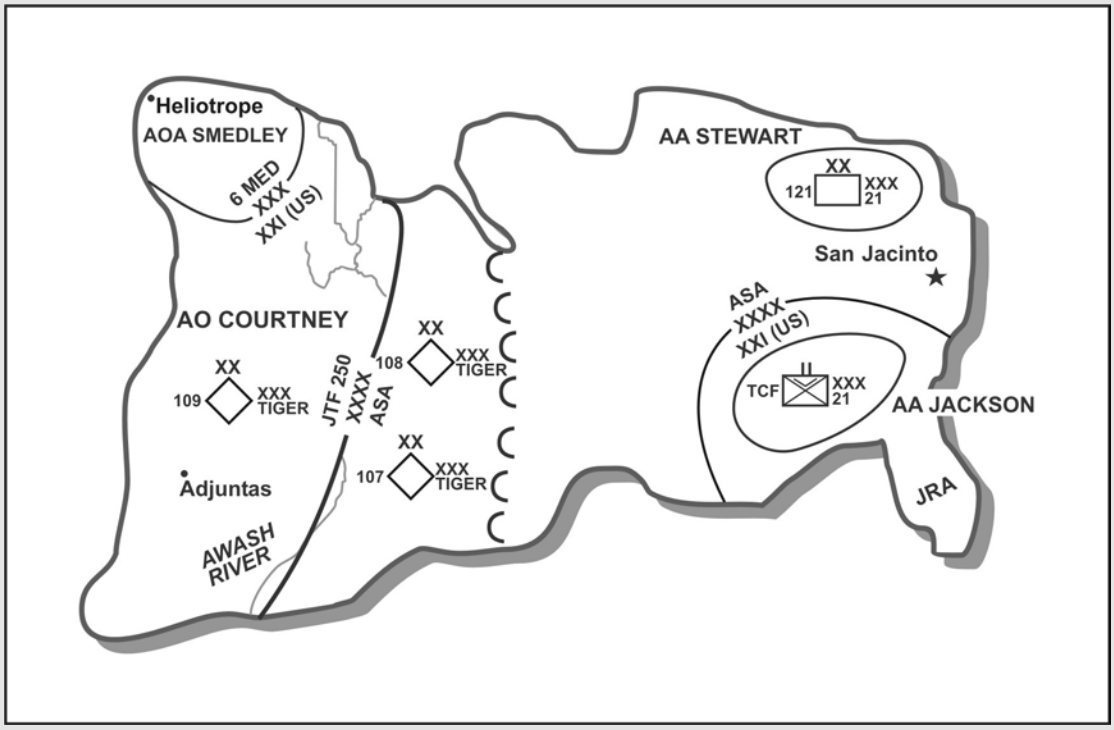


Figure B-1. Joint Operations Area SAN ANGLOS

The ASA is well trained and has participated in exercises with US forces. It could probably reoccupy western San Anglos unassisted; however, its leaders believe that such an action would require extended fighting and result in destruction of the industry and infrastructure. San Anglos also lacks the maritime capability to block reinforcements from Rendova. Therefore, 45 days ago, San Anglos requested US assistance. The Government of San Anglos believes that the US capability to conduct rapid land operations, combined with US sea power, will allow the ASA to quickly overwhelm Rendovan forces and reestablish San Anglos control of the occupied territory. The US President authorized the geographic combatant commander responsible for the area to create and deploy Joint Task Force (JTF) 250 to conduct coalition operations with San Anglos forces. For political reasons, the coalition force has a parallel command structure. A coalition coordination, communications, and integration center (C3IC) is coordinating the operations of JTF 250 and San Anglos forces. Several JTF IO, including psychological operations (PSYOP) and a military deception (MD) operation, are underway.

MDMP TASK 1—RECEIPT OF MISSION

B-1. When a mission is received or deduced, the commander and staff conduct an initial assessment. The commander issues initial guidance and the staff prepares and issues a warning order (WARNO). The JTF 250 operation order (OPORD) illustrated in figure B-2 contains the initial instructions to XXI Corps.

[Heading information omitted]

HEADING/**TASK ORGANIZATION**//

/**UNITDES**	/**UNITLOC**	/**CMNTS**
XXI CORPS	SAN ANGLOS	ARFOR
1ST AEF	SAN JACINTO	AFFOR
COMBATGRU16	STRAIT OF DAWARO	NAVFOR
6TH MEB	AFLOAT	MARFOR

GENTEXT/**SITUATION**/

1. **GENERAL SITUATION**.

A. **ENEMY FORCES**. The invasion force is the Rendovan Tiger Corps, consisting of three motorized divisions, the 107th, 108th, and 109th. Two divisions face the ASA along the line of contact. The third occupies the conquered territory. Tiger Corps has established defensive positions and is awaiting reinforcements from the port of RSOSCHKOSH. Rendovan propaganda is emphasizing alleged US “neocolonialism” and condemning the leaders of San Anglos as “campradore collaborators.”

B. **FRIENDLY FORCES**. ASA attacks D-day, H-hour to destroy the 107th and 108th Divisions; links up with XXI Corps vicinity AWASH River; prepares to assume control of AO COURTNEY and AOA SMEDLEY.

GENTEXT/**MISSION**/

2. JTF 250 attacks D-day, H-hour to clear AO COURTNEY and restore the territorial integrity of San Anglos; seize HELIOTROPE and clear AOA SMEDLEY to prevent movement of Rendovan reinforcements into San Anglos; links up with ASA vicinity AWASH River; assists Government of San Anglos in reestablishing order and basic services; on order passes control of AO COURTNEY and AOA SMEDLEY to ASA.

GENTEXT/**EXECUTION**/

3. **CONCEPT OF OPERATIONS**.

A. **Phase I**: NAVFOR/6th MEB conducts amphibious assault to seize HELIOTROPE and clear AOA SMEDLEY. XXI Corps clears AO COURTNEY; links up with ASA vicinity of the AWASH River; links up with 6th MEB. The coalition decisive operation is the ASA attack. The JTF 250 decisive operation is the XXI Corps operation. The end state is the destruction or capture of all Tiger Corps forces.

B. **Phase II**: JTF 250 supports San Anglos civil authorities restoring order and civil services.

Figure B-2. Joint Task Force 250 Operation Order

C. **Phase III**: JTF 250 passes control of AO COURTNEY/AOA SMEDLEY to ASA.

D. **Military Deception**. JTF 250 deception story is that JTF forces will conduct an amphibious and air assault to seize RSOSCHKOSH and secure a beachhead for follow-on operations by XXI Corps forces using northern San Anglos as a staging area.

4. **ARFOR**.

A. **Phase I**.

(1) Clear AO COURTNEY.

(2) Link up with ASA forces vicinity AWASH River.

(3) Link up with 6th MEB vicinity HELIOTROPE.

(4) Provide IO support to 6th MEB for amphibious assault.

(5) Assume JFLCC responsibilities upon linkup with 6th MEB.

B. **Phase II**: Support Government of San Anglos in restoring order and civil services in AO COURTNEY and AOA SMEDLEY.

C. **Phase III**: Pass control of AO COURTNEY and AOA SMEDLEY to ASA.

D. **Military Deception**. Portray preparation for air assault of RSOSCHKOSH to support the JTF 250 deception story.

5. **AFFOR** (all phases).

A. Gain and maintain air superiority.

B. Prevent air movement of Rendovan forces and supplies from RSOSCHKOSH to HELIOTROPE.

C. Support coalition ground operations with CAS and intratheater logistics.

D. Maintain control of air lines of communications.

E. Assume JFACC responsibilities upon linkup with 6th MEB.

6. **NAVFOR** (all phases).

A. Conduct sea control operations in Strait of Dawaro.

B. Prevent sea movement of Rendovan forces and supplies from RSOSCHKOSH to HELIOTROPE.

C. Portray preparations for amphibious assault of RSOSCHKOSH.

D. Support MARFOR amphibious assault of HELIOTROPE.

E. Support coalition ground operations with logistics.

F. Maintain control of sea lines of communications.

G. Transfer control of 6th MEB to ARFOR upon linkup with XXI Corps.

Figure B-2. Joint Task Force 250 Operation Order (continued)

7. **MARFOR**.

A. Conduct amphibious assault to seize HELIOTROPE to prevent its use by Rendovan reinforcements from RSOSCHKOSH.

B. Clear AOA SMEDLEY.

C. Link up with XXI Corps. CHOP from NAVFOR to JFLCC at linkup.

8. **COORDINATING INSTRUCTIONS**.

A. The name of this operation is FRIED ANCHOR.

B. This OPORD is effective for planning upon receipt and execution in 72 hours.

C. Do not execute PSYOP or EW on frequencies that might cause interference with local civil communications.

D. Minimize damage to civilian infrastructure.

E. Maintain support of the local populace.

GENTEXT/**ADMIN AND LOG**/

9. [omitted]

GENTEXT/**COMMAND AND SIGNAL**/

10. [omitted]

AKNLDG/Y//

DECL/OADR//

Figure B-2. Joint Task Force 250 Operation Order (continued)

INITIAL ASSESSMENT AND COMMANDER'S INITIAL GUIDANCE

B-2. When the commander and staff have finished their initial assessment, the commander issues initial guidance. The XXI Corps commander issues the initial guidance in figure B-3.

H-hour is in 72 hours. That gives us time to do a full-blown MDMP. I want to issue the OPORD in 24 hours. Give me a mission analysis briefing in 6 hours. Plan to begin the war game in 12 hours.

Make sure our ASA and 6th MEB liaison teams have everything they need.

G-2, identify the locations of the 107th and 108th Division reserves. Locate any battalion-sized 109th Division concentrations. G-3, initiate reconnaissance to fill gaps left by higher-level assets. Avoid any operations that would reveal the XXI Corps mission.

Minimize any movements. I want to execute from our current locations if possible.

Figure B-3. XXI Corps Commander's Initial Guidance

When movements are necessary, conceal them or portray them as preparations for an air assault on RSOSCHKOSH.

G-3, plan the operation as an air assault by the 121st Division. Consider both a single and a double envelopment. I don't want to overfly the ASA FLOT.

FSCOORD, find out what JFACC and NAVFOR can do for us in the JSEAD area. An air assault will take unacceptable losses without their support, and we need them to reinforce our artillery once we're on the ground. We are the JTF decisive operation, and we need their help on this one.

G-5, focus your planning on Phase II. G-3, I want a seamless transition from offensive to support operations. G-7, support him with PSYOP and any other IO assets and resources you can muster. I want to minimize civilian casualties. G-5, G-7, look at ways to make this happen.

G-7, give me a recommendation on when to shift resources from the MD operation to the air assault. I want to achieve operational surprise, but I also need as many of those resources as I can get for the air assault. Look at ways to portray the objective of the air assault as RSOSCHKOSH. Coordinate this with NAVFOR.

G-7, IO is key to our success. We need to achieve surprise and we need to be able to talk. You have the lead on both of those tasks. Focus on the 109th Division, but look at the entire Tiger Corps C2 system. Coordinate any IO that might affect ASA operations through the C3IC. Here are the initial EEFI:

- *The XXI Corps mission and concept of operations.*
- *The identity and locations of the XXI Corps critical C2 system nodes.*
- *The identity and locations of the TAC and main CPs of the XXI Corps, its subordinate divisions, the Corps Artillery and the Corps Support Command.*
- *The location of the INFOSYS nodes for 21st CAB CP and its subordinate battalion CPs.*

Figure B-3. XXI Corps Commander's Initial Guidance (continued)

WARNING ORDER

B-3. Based on the initial assessment and initial guidance, the XXI Corps staff issues the WARNO illustrated in figure B-4.

[heading omitted]

WARNING ORDER 21-01

References. JTF 250 OPORD 01, DTG; [map sheets]; operation overlay [see figure B-1, page B-2]

Time Zone Used throughout the Order: Zulu

Figure B-4. First XXI Corps Warning Order (extract)

Task Organization.

121st ID	21st Signal Bde	Corps Artillery
21st CAB	27th ACR	1st Bn, 19th PSYOP Grp
21st MI Bde	365th CA Bde	21st Public Affairs Det

1. **SITUATION**.

a. **Enemy forces**. Tiger Corps controls the western third of San Anglos. Two divisions (the 107th and 108th) face ASA forces. One (the 109th) serves as the occupation force for western San Anglos.

b. **Friendly forces**. ASA attacks D-day, H-hour to destroy Tiger Corps along the line of contact; links up with XXI Corps vicinity AWASH River. 6th MEB conducts amphibious assault to seize HELIOTROPE to prevent Rendovan reinforcement from RSOSCHKOSH; clears AOA SMEDLEY; links up with XXI Corps. Coalition decisive operation is ASA attack. JTF 250 decisive operation is XXI Corps operations. JFACC and NAVFOR support XXI Corps with JSEAD, AI, and CAS.

c. **Attachments and detachments**. [omitted]

2. **MISSION**. TBD.

3.**EXECUTION**.

Intent. TBD.

a. **Concept of operations**. XXI Corps conducts air assault D-day, H-hour to seize forward operating bases in western San Anglos; clears AO COURTNEY; links up with ASA vicinity AWASH River; links up with 6th MEB; supports Government of San Anglos in restoring order and civil services.

b. **Tasks to maneuver units**.

(1) [Initial movement and reconnaissance instructions are omitted.]

(2) 121st ID. Prepare to execute air assault and clear AO COURTNEY.

c. **Tasks to combat support units**.

(1) [Initial movement and reconnaissance instructions are omitted.]

(2) 21st CAB. Prepare to support air assault by 121st ID.

(3) 365th CA Bde. Prepare to assist San Anglos civil authorities in reestablishing order and services in AO COURTNEY and AOA SMEDLEY.

d. **Coordinating instructions**.

(1) Initial Time Line. H-hour is DTG [72 hours from receipt of JTF OPORD]; expect OPORD by DTG [24 hours from receipt of JTF OPORD]; rehearsal will be held at [location] at DTG.

(2) EEFI.

(a) The XXI Corps mission and concept of operations.

Figure B-4. First XXI Corps Warning Order (extract) (continued))

(b) The identity and locations of the XXI Corps critical C2 system nodes.

(c) The identity and locations of the TAC and main CPs of the XXI Corps, its subordinate divisions, the Corps Artillery, and the Corps Support Command.

(d) The location of the INFOSYS nodes for 21st CAB CP and its subordinate battalion CPs.

(3) Deception guidance.

(a) Continue current MD operations.

(b) Conceal all movements or portray them as preparations for an air assault on RSOSCHKOSH.

(4) Risk guidance. [omitted]

4. **SERVICE SUPPORT**. [omitted]

5. **COMMAND AND SIGNAL**. [omitted]

ACKNOWLEDGE: [authentication omitted]

Figure B-4. First XXI Corps Warning Order (extract) (continued))

MDMP TASK 2—CONDUCT MISSION ANALYSIS

B-4. During mission analysis, staffs define the tactical problem and begin to determine feasible solutions. Mission analysis produces the restated mission, initial commander's intent, commander's guidance, and at least one WARNO. The G-7 ensures each of these products considers IO factors and provides IO input to the other tasks. The major G-7 mission analysis products are the initial IO mission statement and an updated IO estimate.

Mission Analysis Tasks

- Analyze the higher headquarters order
- Conduct IPB
- Determine specified, implied, and essential tasks
- Review available assets
- Determine constraints
- Identify critical facts and assumptions
- Conduct risk assessment
- Determine initial CCIR
- Determine the initial ISR annex
- Plan use of available time
- Write the restated mission
- Conduct a mission analysis briefing
- Approve the restated mission
- Develop the initial commander's intent
- Issue the commander's guidance
- Issue a warning order
- Review facts and assumptions

ANALYZE HIGHER HEADQUARTERS ORDER

B-5. Mission analysis begins with a thorough examination of the XXI Corps OPORD in light of the commander's initial guidance. There is no formal IO product for this task. Its purpose is for all to obtain a clear understanding of the mission and information relating to it, especially the higher commander's intent.

CONDUCT INITIAL INTELLIGENCE PREPARATION OF THE BATTLEFIELD

B-6. The G-7 provides IO input, including IO-related high-value targets, to the G-2 for intelligence preparation of the battlefield (IPB). The portions of IPB relating to IO become parts of paragraph 2 of the IO estimate (see figure B-5).

2. **SITUATION AND CONSIDERATIONS**.

a. **Characteristics of the AO and information environment**.

(1) Weather. Storms that would preclude air assault operations are infrequent at this time of year.

(2) Terrain and physical environment. [omitted]

(3) Information environment.

(a) Intense media interest in JTF 250 operations exists due to the long-standing relationship between the US and both Rendova and San Anglos. International media presence on San Anglos is steadily increasing.

(b) San Anglos has a free press. Hard-hitting investigative reporting is valued.

(c) Most San Anglos homes have radios. Virtually all citizens have access to televisions. San Anglos is within the broadcast footprint of major Rendovan radio and television outlets. San Anglos broadcast media continue to operate.

(d) San Anglos has allowed most foreign journalists into the country.

(4) Probable adversary picture of friendly forces. [omitted]

b. **Enemy Forces**. The major force opposing XXI Corps is the 109th Division of the Tiger Corps. The 107th and 108th Divisions face the ASA. The 109th Division is the occupation force for western San Anglos. It is widely dispersed, with no force concentration larger than a battalion. The brigade-sized reserves of the 107th and 108th Divisions are close enough to AO COURTNEY to be employed against XXI Corps.

(1) Decisionmakers and decisionmaking process. Commander, Tiger Corps is the deception target. He must be made to believe that the ASA will continue to defend and that XXI Corps is preparing to exploit an amphibious assault on RSOSHKOSH.

(2) INFOSYS strengths and vulnerabilities. Critical Rendovan C2 systems and ISR nodes include the CPs of the Tiger Corps and its divisions; artillery-associated radars and target processing systems; ground control stations for the divisional UAV companies; and divisional signal nodes (primarily line-of-sight and troposcatter multichannel systems, and their control centers).

(3) IO capabilities, dispositions, composition, and strengths.

(a) Tiger Corps and its divisions receive operational-level intelligence and targeting support from Special Purpose Forces and agents.

(b) 409th Radio Electronic Combat (REC) Battalion (109th Division) can detect, locate, and jam AM and FM radio communications in the HF-VHF frequency bands.

Figure B-5. Paragraphs 2a and 2b, Information Operations Estimate

109th REC battalion can conduct CNA. Each division also has an organic REC company with similar capabilities minus CNA.

(c) 409th Public Information Company (109th Division) can produce and disseminate propaganda. Brigades do not have a similar capability.

(d) Rendovan ISR capabilities are robust, multidiscipline, and multispectral. They consist of both ground-based and airborne systems comparable to those of Western European nations.

(e) Tiger Corps is supported by a sophisticated fire support capability, including tube artillery and an attack helicopter battalion. The brigades of its divisions have 120 mm mortars. Each division has an artillery battalion with medium-range, self-propelled cannon and a multiple rocket launcher battery. The 109th Division's artillery and multiple rocket launchers are supporting the 107th and 108th Divisions. The 109th Division's brigades retain control of their mortars.

(f) HVT are corps, division, and brigade CPs, and supporting communications nodes; air defense- and artillery-associated radars, and target-processing systems; REC assets; and the local civilian populace.

(g) The Rendovans are adept at using the national and international media to exploit political and military actions for their propaganda potential.

(h) Rendovan air defense is highly sophisticated; has excellent, redundant INFOSYS; and has very good long-range, low-altitude detection capabilities. Its highly centralized command structure is its most significant weakness.

(4) Likely IO COAs.

(a) COA #1—Most likely. Tiger Corps commander is surprised by the air assault. He reacts by counterattacking with one or both of the frontline divisions' reserves.

(b) COA #2—Most dangerous. Tiger Corps commander discovers the deception plan and prepares to defeat the air assault. Plans could include positioning artillery, air defense, and ground forces to attack possible LZs, and making arrangements to flood LZs with dislocated civilians.

Figure B-5. Paragraphs 2a and 2b, IO Estimate (continued)

B-7. The G-7 examines the results of the initial IPB to determine the critical nodes of the Tiger Corps C2 system. These may include command posts, (CPs) C2 system nodes, networks, and information systems (INFOSYS) critical to the Tiger Corps and 109th Division commanders' decisionmaking processes. The analysis identifies information gaps. The G-7 submits IO information requirements (IRs) to fill these gaps to the G-2. The G-7 also requests information on Tiger Corps intelligence, surveillance, and reconnaissance (ISR) assets to better determine enemy capabilities and vulnerabilities that may affect the air assault. This information includes Tiger Corps's ability to collect and exploit information from the XXI Corps C2 system and Tiger Corps air defense systems' ability to counter JTF electronic warfare (EW) capabilities. IO-cell members—especially the PSYOP, civil-military operations (CMO), and public affairs (PA) representatives—identify how best to influence the attitudes and actions of the civilian populace in the area of

operations (AO). This effort results in additional IO IRs concerning target audience analysis for PSYOP. These are submitted to the G-2. As answers to these IO IRs arrive, they are added to paragraph 2 of the IO estimate.

DETERMINE SPECIFIC, IMPLIED, AND ESSENTIAL TASKS

B-8. Concurrently with the initial IPB, the staff analyzes the JTF OPORD to identify specified, implied, and essential tasks assigned to XXI Corps. Some of these tasks may require IO to accomplish. For the G-7, this task comprises identifying these IO-related specified tasks in the higher headquarters OPORD, developing IO-related implied tasks that support accomplishing the mission, and assembling the critical asset list (see figure B-6).

IO-Related Specified Tasks

- Portray preparation for an air assault of RSOSCHKOSH.
- Provide IO support to 6th MEB for amphibious assault.
- (Essential task) Support Government of San Anglos in restoring order and civil services in AO COURTNEY and AOA SMEDLEY.

IO-Related Implied Tasks

- Prevent compromise of the operation.
- Protect XXI Corps C2.
- Disrupt Tiger Corps and 109th Division ADA, ISR, C2, and targeting systems during critical periods of the operation.
- Minimize civilian interference in AO COURTNEY.

Critical Asset List

- Corps area common-user network (voice and data).
- Tactical-to-strategic theater communications interface points.
- UAV-SR (Hunter).
- Quick Fix.
- Guardrail.

Figure B-6. Information-Operations-Related Tasks and Critical Assets

B-9. One of the IO-related tasks assigned to XXI Corps is, Portray preparation for an air assault of RSOSCHKOSH. This task supports the JTF deception operation. The JTF deception operation targets Rendovan national decisionmakers. It is attempting to convince them that the US is using San Anglos as a staging area for an invasion of Rendova that will be spearheaded by the 6th Marine Expeditionary Brigade (MEB), which is off shore in the Strait of Dawaro. It is supported by a national-level PSYOP campaign that is emphasizing the US President's "desire to strike at the root of the problem" (by invading Rendova itself), "rather than nibbling around the edges" (conducting combat operations on San Anglos). The XXI Corps military deception (MD) operation is complementing the JTF and national deception operations by portraying XXI Corps as preparing for an air assault across the Strait of Dawaro. Convincing the Tiger Corps and 109th Division commanders that this portrayal is the actual situation is an MD task that supports the IO-

related implied task, Prevent compromise of the operation. The military deception officer (MDO) is responsible for overseeing the corps MD operation and synchronizing it with the JTF deception operation. MD planning proceeds concurrently with planning for the overall operation.

B-10. Supporting the Government of San Anglos in restoring order and civil services in AO COURTNEY and AOA SMEDLEY is mainly a CMO task. However, it might involve such IO elements/related activities as public affairs and PSYOP. The G-7 and G-5 coordinate IO aspects of this task with the G-3.

REVIEW AVAILABLE ASSETS

B-11. From the JTF order, the G-7 identifies joint assets in the task organization that might be available for IO support to XXI Corps. The G-7 also reviews the XXI Corps standing operating procedure (SOP) to identify available assets and resources that can be employed in an IO role. These resources form subparagraphs 2c(2) and (3) of the IO estimate (see figure B-7).

2. **SITUATION AND CONSIDERATIONS**.

a. **Characteristics of the area of operations and information environment**. [omitted; see figure B-5, page B-9]

b. **Enemy Forces** [omitted; see figure B-5, page B-9].

c. **Friendly Forces**.

(1) **IO concept of support to each COA**. [developed during COA development].

(2) **Current status of IO assets**.

(a) EW.

(i) 21st MI Bde.

(ii) 21st Signal Bde.

(b) PSYOP.

(i) XXI Corps PSYOP Support Element.

(ii) 1st Battalion, 19th PSYOP Grp.

(c) PA.

(i) XXI Corps PAO.

(ii) 21st PA Det.

(d) Physical destruction.

(i) XXI Corps maneuver units.

(ii) XXI Corps Artillery.

(iii) 21st CAB.

(e) CMO. 365 CA Bde.

(3) **Current status of IO resources**.

(a) Special Operations Command and Control Element (SOCCE) liaison team.

(b) 1st Information Operations Command (Land).

(i) Field support team (attached).

(ii) Vulnerability assessment team (attached).

Figure B-7. Paragraph 2c, IO Estimate—IO Asset and Resources Identification

(c) JFACC.
(i) EW [list support available].
(ii) PSYOP [list support available]
(iii) Physical destruction [list support available].
(d) MARFOR.
(i) EW [list support available]
(ii) Physical destruction [list support available]
d. **OPSEC**. [omitted]
e. **Assumptions**. [omitted; see figure B-9, page B-13]

Figure B-7. Paragraph 2c, IO Estimate—IO Asset and Resources Identification (continued)

DETERMINE CONSTRAINTS

B-12. The G-7's review of the JTF order also produces a list of constraints that may affect IO (see figure B-8). These are placed in either the IO concept of support or coordinating instructions of the IO annex.

- Maintain support of the local populace
- Minimize damage to the civilian infrastructure
- Do not execute PSYOP or EW on frequencies that might cause interference with local civil communications

Figure B-8. Constraints Affecting IO

IDENTIFY CRITICAL FACTS AND ASSUMPTIONS

B-13. Throughout mission analysis, the G-7 identifies critical IO-related facts and assumptions. Facts are placed in the subparagraph of the IO estimate that that concerns them (usually 2a, 2b, or 2c). Assumptions are placed in subparagraph 2e. Figure B-9 shows the assumptions the G-7 makes based on the initial analysis of the JTF order and XXI Corps AO.

2. **SITUATION AND CONSIDERATIONS**.

a. Characteristics of the AO and information environment. [omitted; see figure B-5, page B-9].

b. Enemy Forces. [omitted; see figure B-5, page B-9]

c. Friendly Forces. [omitted; see figure B-7, page B-12].

d. OPSEC. [omitted; determined during risk assessment]

e. Assumptions.

Figure B-9. Paragraph 2d, IO Estimate—IO-Related Assumptions

(1) Rendovan forces will take advantage of friendly ROE and constraints concerning civilian casualties, and will attempt to employ dislocated civilians to block LZs and clog maneuver routes in the objective area.

(2) JSEAD support from JTF air and naval assets will be available and effective.

(3) Rendovan IO-associated capabilities will attack key XXI Corps communications and ISR systems/nodes in an effort to degrade friendly C2 and intelligence at critical points in the operation.

Figure B-9. Paragraph 2d, IO Estimate—IO-Related Assumptions (continued)

CONDUCT RISK ASSESSMENT

B-14. During mission analysis, the G-7 assesses primarily OPSEC- and C2-related hazards. The G-7 uses the technique that FM 100-14 prescribes for assessing hazards associated with tactical risk to assess these hazards. Figure B-10 shows an extract of an example of the work sheet the G-7 used to assess OPSEC- and C2-related hazards.

Mission: TBD. Concept of operations: XXI Corps conducts air assault D-day, H-hour to seize forward operating bases in western San Anglos; clears AO COURTNEY; links up with ASA vicinity AWASH River; links up with 6th MEB; supports Government of San Anglos in restoring order and civil services.

1 EEFI/C2 Category/Critical Asset	2 OPSEC/C2 Vulnerability	3 Assess Hazards	4 Develop Controls	5 Determine Residual Risk	6 Implement Controls
[EEFI] The XXI Corps mission and concept of operations	[List associated OPSEC vulnerabilities]	[Assess each OPSEC vulnerability]	[List controls to reduce the risk associated with each vulnerability]	[List residual risk associated with each OPSEC vulnerability]	[List means the G-7 will use to assess the success of controls. Include IO IRs, if any]
[C2-related] Tactical-to-strategic theater communications interface points	[List associated hazards]	[Assess each hazard]	[List controls for each hazard]	[List residual risk associated with each hazard]	[List means the G-7 will use to assess the success of controls. Include IO IRs, if any]
[Critical asset] UAV-SR (Hunter)	[List associated hazards]	[Assess each hazard]	[List controls for each hazard]	[List residual risk associated with each hazard]	[List means the G-7 will use to assess the success of controls. Include IO IRs, if any]

Figure B-10. Initial Assessment of IO-Related Hazards (extract)

B-15. Column 1 lists the essential elements of friendly information (EEFI), C2 systems, and critical assets that the G-7 has identified. Using the OPSEC process, the G-7 identifies OPSEC vulnerabilities associated with each EEFI element. In coordination with the G-3 and G-6, the G-7 determines the hazards that could cause the loss of each INFOSYS/critical asset. These are listed in column 2. The G-7 uses a risk assessment matrix similar to the one at figure B-11, page B-15, to estimate the chance of a hazard incident

occurring if no controls other than those established by SOP are implemented. That probability and the severity of an incident determine the risk associated with each hazard. That risk is entered in Column 3 for each hazard.

B-16. The following paragraphs describe the logic the G-7 followed in assessing one EEFI element and one C2-related vulnerability.

- **Compromise of the XXI Corps mission and concept of operations** could result in a loss of surprise. The G-3 estimates that this situation could result in mission failure (a catastrophic effect). Following the OPSEC process, the G-7 identifies OPSEC indicators that could reveal this information and determines which of them Tiger Corps is capable of acquiring. These are OPSEC vulnerabilities. With G-2 assistance, the G-7 estimates the likelihood that Rendovan ISR operations will acquire each vulnerability. The G-2 and G-7 then estimate the probability that the Rendovan intelligence system will acquire and process enough of the vulnerabilities to deduce the corps mission and concept of operations. The G-7 uses that estimate to enter the risk assessment matrix and determine the risk associated with this EEFI element.
- **Tactical-to-strategic theater communications interface points** have been designated as critical C2 assets. With the G-6, the G-7 estimates the effect that losing each node or system would produce. With the G-2, the G-7 estimates the likelihood of each being lost. Based on these two estimates, the G-7 determines the overall risk to this system.

Severity of Hazard Incident	Probability of Hazard Incident Occurring				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	E	E	H	H	H
Critical	E	H	H	M	L
Marginal	H	M	M	L	L
Negligible	M	L	L	L	L

E–Extremely High Risk **H**–High Risk **M**-Moderate Risk **L–**Low Risk
See FM 100-14 for severity and probability descriptions.

Figure B-11. Risk Assessment Matrix

B-17. The G-7 then develops controls to manage these hazards (entered in column 4) and means of assessing the controls (entered in column 5), and determines the residual risk associated with each hazard (entered in column 6). The G-7 may compute an overall risk for each EEFI element, C2 hazard, and critical asset, if appropriate. The G-7 coordinates controls with other staff sections as necessary. Controls that require IO tasks to implement are added to the IO input matrix for the course of action (COA). Controls that require significant resources to implement are presented to the commander for approval. IO IRs that support assessment of controls are submitted to the G-2.

DETERMINE INITIAL COMMANDER'S CRITICAL INFORMATION REQUIREMENTS

B-18. During mission analysis, the G-7 recommends as commander's critical information requirements (CCIR) any IRs dealing with information the commander needs to make critical decisions on employing IO during the upcoming operation. The G-7 recommends that the commander include the IO

IRs listed in figure B-12 with the CCIR. The G-7 submits them to the G-3 as specified in the unit SOP. The G-7 refines IO IRs and tracks their status throughout the operation.

Priority Intelligence Requirements

- What and where are the critical INFOSYS nodes associated with the 109th Division and its subordinate maneuver, air defense, and artillery assets?
- What and where are the critical INFOSYS nodes associated with Tiger Corps maneuver, air defense, and artillery assets within supporting distance of the 109th Division?
- Will the 109th Division employ dislocated civilians to disrupt XXI Corps operations in the objective areas? How will they do this?
- What ISR assets will Tiger Corps/109th Division forces use to identify the nature and objectives of this operation? What are their capabilities and vulnerabilities? Where are they deployed?

Friendly Force Information Requirements

- Loss or degradation of critical XXI Corps INFOSYS nodes or networks, specifically the XXI Corps airborne CP and TAC CP, and the C2 and fire support nets of the 121st ID and the 21st CAB
- Damage or destruction of civil infrastructure in the objective area caused by XXI Corps operations
- Death or injury of civilians in the objective area due to XXI Corps operations

Figure B-12. IO IRs Recommended as CCIR

DETERMINE THE INITIAL INTELLIGENCE, RECONNAISSANCE, AND SURVEILLANCE ANNEX

B-19. The G-2 incorporates IO IRs from the G-7 into the collection plan and ISR taskings. The G-3 prepares the initial ISR annex and issues the orders necessary to begin collection.

PLAN USE OF AVAILABLE TIME

B-20. At this point, the G-3 refines the initial time plan developed at receipt of mission. The G-7 makes sure the G-3 considers any IO tasks that require a long lead-time to accomplish. Upon receiving the revised time plan, the G-7 refines the initial IO time allocation plan.

WRITE THE RESTATED MISSION

B-21. The G-3 develops the proposed restated mission based on the essential tasks. The G-7 provides IO input based on the current IO estimate. The restated mission must include IO-related essential tasks, if any. Figure B-13 shows the XXI Corps restated mission.

XXI Corps attacks D-day, H-hour to clear AO COURTNEY; links up with ASA forces vicinity AWASH River, links up with 6th MEB vicinity HELIOTROPE; supports Government of San Anglos authorities in establishing order and providing basic services.

Figure B-13. XXI Corps Restated Mission

CONDUCT A MISSION ANALYSIS BRIEFING AND APPROVE THE RESTATED MISSION

B-22. Time permitting, the staff briefs the commander on the results of its mission analysis. The G-7 provides the input shown in figure 5-4, page 5-18). After the mission analysis briefing, the commander approves or alters the re-stated mission.

DEVELOP THE INITIAL COMMANDER'S INTENT

B-23. At the end of the mission analysis briefing, the XXI Corps commander issues the initial commander's intent (see figure B-14).

Key tasks XXI Corps must accomplish are—

- Clear AO COURTNEY.
- Link up with ASA.
- Link up with 6th MEB.
- Support San Anglos civil authorities in restoring order and basic services.

The tempo will be fast. Shock the Rendovan commander into inaction and destroy his forces before they have time to react to our attack or damage any of the civilian infrastructure. Anticipate beginning support operations NLT H + 48.

Figure B-14. Initial XXI Corps Commander's Intent

ISSUE THE COMMANDER'S GUIDANCE

B-24. After approving the restated mission and stating his intent, the commander provides the staff with enough additional guidance to focus staff planning activities. Commanders may give guidance for IO separately or as part of their overall initial guidance. In this case, the XXI Corps commander issues the separate IO guidance shown in figure B-15. Based on this guidance, the G-7 prepares the initial IO mission statement.

[IO Objectives]

Two defensive IO objectives are apparent:

- *Prevent compromise of XXI Corps mission and concept of operations.*
- *Protect XXI Corps C2.*

Develop offensive IO objectives to support each COA.

[OPSEC Planning Guidance]

EEFI remain the same. Notify the G-3 if you identify additional EEFI. Disseminate them by WARNO.

Continue with OPSEC measures prescribed in the SOP. Synchronize OPSEC operations with MD operations. Focus on any OPSEC vulnerabilities that would reveal our actual mission.

Figure B-15. XXI Corps Commander's IO Guidance

[Military Deception Guidance]

The deception objective remains to convince the Tiger Corps commander that we are going to attack Rendova proper. Continue our ongoing MD operation. Inform me immediately of any possible compromises.

[Targeting Guidance]

- *Destroy ADA systems.*
- *Degrade Rendovan ISR systems. Priority to ADA systems.*
- *Disrupt Rendovan C2 nets.*
- *Exploit Rendovan intelligence nets.*

[Psychological Operations Guidance]

Focus PSYOP on influencing civilians to remain in their homes during the operation.

[Public Affairs Guidance]

Use PA to favorably influence the population in the AO and worldwide. Emphasize the lead role of the ASA and tell the truth: that we are here to assist a well-trained army accomplish a worthwhile mission.

Figure B-15. XXI Corps Commander's IO Guidance (continued)

ISSUE A WARNING ORDER

B-25. Immediately after the commander gives his guidance, the G-3 sends subordinate and supporting units a WARNO (see figure B-16). The G-7 provides IO input to the G-3 for inclusion in the WARNO. This input includes, as a minimum, the initial IO mission statement, the OPSEC planning guidance, and MD planning guidance.

[heading omitted]

WARNING ORDER 21-02

References. JTF 250 OPORD 01, DTG; XXI Corps WARNO 21-01, DTG; [map sheets]

Time Zone Used throughout the Order: Zulu

1. **SITUATION**.

   a. **Enemy forces**. Current intelligence summary.

   b. **Friendly forces**. No change.

   c. **Attachments and detachments**. [omitted]

2. **MISSION**. XXI Corps attacks D-day, H-hour to clear AO COURTNEY, link up with ASA forces vicinity AWASH River, and link up with 6th MEB vicinity HELIOTROPE; supports Government of San Anglos authorities in establishing order and providing basic services.

B-16. Second XXI Corps Warning Order (extract)

3. **EXECUTION**.

Intent. Key tasks XXI Corps must accomplish are (1) clear AO COURTNEY, (2) link up with the ASA (3) link up with 6th MEB, and (4) support San Anglos civil authorities in restoring order and basic services. The tempo will be fast. Shock the Rendovan commander into inaction and destroy his forces before they have time to react to our attack or damage any civilian infrastructure. Anticipate beginning support operations NLT H + 48.

a. **Concept of operations**.

[(1)–(6) omitted]

(7) **Information Operations**.

(a) **IO mission statement**. IO supports XXI Corps operations by preventing preemption of the air assault, influencing the local population not to interfere in and around the objective areas, and shaping the information environment to support efforts to establish order and provide basic services.

(b) **IO Objectives**.

(1) Prevent compromise of XXI Corps mission and concept of operations.

(2) Protect XXI Corps C2.

(c) **Critical Asset List**.

(1) Corps area common-user network (voice and data).

(2) Tactical-to-strategic theater communications interface points.

(3) UAV-SR (Hunter).

(4) Quick Fix.

(5) Guardrail.

(d) **Targeting Guidance**.

(1) Destroy C2 for ADA systems in AO COURTNEY.

(2) Degrade ISR systems. Priority to ADA systems.

(3) Disrupt C2 nets.

(4) Exploit intelligence nets.

(5) Focus PSYOP on influencing the population to remain in their homes during the operation.

(6) Use PA to favorably influence the population in the AO and worldwide. Emphasize the lead role of the ASA and tell the truth: that we are here to assist a well-trained army accomplish a worthwhile mission.

(e) **Constraints**.

(1) Maintain support of the local populace.

Figure B-16. Second XXI Corps Warning Order (extract) (continued)

(2) Minimize damage to the civil infrastructure.

(3) Do not employ PSYOP or EW assets on frequencies that might cause interference with local civil communications.

b. Tasks to maneuver units.

(1) 121st ID.

(a) Conduct air assault to clear AO COURTNEY.

(b) Prepare to support Government of San Anglos authorities in establishing order and services.

(2) 27th ACR.

(a) Cover west flank of 121st ID.

(b) Link up with ASA vicinity AWASH River.

c. Tasks to combat support units.

(1) 21st MI Bde.

(a) Portray preparations for air and sea movement across the Strait of Dawaro.

(b) Support JTF 250 deception plan.

(2) 21st CAB. DS 121st ID.

d. Coordinating instructions.

(1) CCIR. [only IO IRs shown]

(a) Priority Intelligence Requirements.

(i) What and where are the critical INFOSYS nodes associated with the 109th Division and its subordinate maneuver, air defense, and artillery assets?

(ii) What and where are the critical INFOSYS nodes associated with Tiger Corps maneuver, air defense, and artillery assets within supporting distance of the 109th Division?

(iii) Will the 109th Division employ dislocated civilians to disrupt XXI Corps operations in the objective areas? How will they do this?

(iv) What ISR assets will Tiger Corps/109th Division forces use to identify the nature and objectives of this operation? What are their capabilities and vulnerabilities? Where are they deployed?

(v) Has the Tiger Corps discovered the deception story?

(b) Friendly Force Information Requirements.

(i) Loss or degradation of critical XXI Corps INFOSYS nodes or networks, specifically the XXI Corps airborne CP and TAC CP, and the C2 and fire support nets of the 121st ID and the 21st CAB.

Figure B-16. Second XXI Corps Warning Order (extract) (continued)

(ii) Damage or destruction of civil infrastructure in the objective area caused by XXI Corps operations.

(iii) Death or injury of civilians due to XXI Corps operations in the objective areas due to XXI Corps operations.

(2) **OPSEC Planning Guidance**.

(a) EEFI. No change from Warning Order 21-01.

(b) Provisional OPSEC measures. [omitted]

(3) **Risk Guidance**. [omitted]

(4) **Deception Guidance**. The deception objective remains to convince the Tiger Corps commander that we are going to attack Rendova proper. Continue our ongoing MD operation. Report any possible compromises.

4. **SERVICE SUPPORT**. [omitted]

5. **COMMAND AND SIGNAL**. [omitted]

ACKNOWLEGE: [authentication omitted]

Figure B-16. Second XXI Corps Warning Order (extract) (continued)

REVIEW FACTS AND ASSUMPTIONS

B-26. Throughout the MDMP, the G-7 periodically reviews the IO facts and assumptions to ensure their comprehensiveness and validity. The restated mission, updated commander's guidance, and initial commander's intent form the basis of this review. These current facts and assumptions are part of the IO running estimate. The G-7 keeps them in mind during COA development.

MDMP TASK 3—COURSE OF ACTION DEVELOPMENT

B-27. After receiving the commander's initial guidance, the staff develops COAs for analysis and comparison. The G-7 ensures that the staff considers IO throughout this task and develops an IO concept of support and other IO products for each COA. The following paragraphs discuss G-7 products developed to support one COA. Time permitting, the G-7 develops similar products for each COA.

COA Development Tasks

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

ANALYZE RELATIVE COMBAT POWER

B-28. IO applies the information element of combat power. The G-7 makes sure that the staff includes IO assets and resources as it analyzes friendly and adversary combat power.

GENERATE OPTIONS

B-29. Based on the commander's guidance and the relative combat power of friendly and adversary forces, the staff generates options for COA development. The G-7 makes sure the staff considers IO factors when it selects COAs from these options. The following paragraphs illustrate development of one COA.

ARRAY INITIAL FORCES

B-30. The G-7 ensures that planners consider IO capabilities and available IO resources when determining forces required for the operation. IO-capable forces are drawn from the list of IO assets and IO resources identified during mission analysis. These are listed in paragraph 2c of the IO estimate (see figure B-7, page B-12). The G-7 also ensures the staff considers the deception story when arraying forces.

DEVELOP THE CONCEPT OF OPERATIONS

B-31. The concept of operations describes how the arrayed forces will accomplish the mission. Figure B-17 shows the COA and COA sketch for Phase I of XXI Corps COA #1. The COA and COA sketch are products of the final COA development task. They are placed here for clarity.

XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.

Decisive. The decisive operation is destruction of all 109th Division forces in detail by simultaneous attacks throughout AO COURTNEY by the 121st Division and 21st CAB attack aviation, supported JTF 250 air and naval fires (JSEAD, AI, and CAS).

Shaping. The intent of shaping operations is to prevent 109th Division forces from massing combat power, to include receiving reinforcement from Tiger Corps or the 107th and 108th Divisions.

21st MI Bde. Portray preparations for air assault across Strait of DAWARO; terminate on order. Conduct EA and nonlethal SEAD against 109th Division C2 system. UAV and remote sensors monitor locations/movements of Tiger Corps and 107th and 108th Division reserves; report movements to 27th ACR.

21st CAB (–). Provide lift for air assault and for 121st ID operations in AO COURTNEY.

27th ACR. Cover 121st ID east flank; link up with ASA vicinity AWASH River.

365th CA Bde. Influence civilians in AO COURTNEY to comply with Government of San Anglos stay-put policy.

Corps Artillery. Reinforce 121st DIVARTY for SEAD; on order, place one FA brigade DS to 27th ACR.

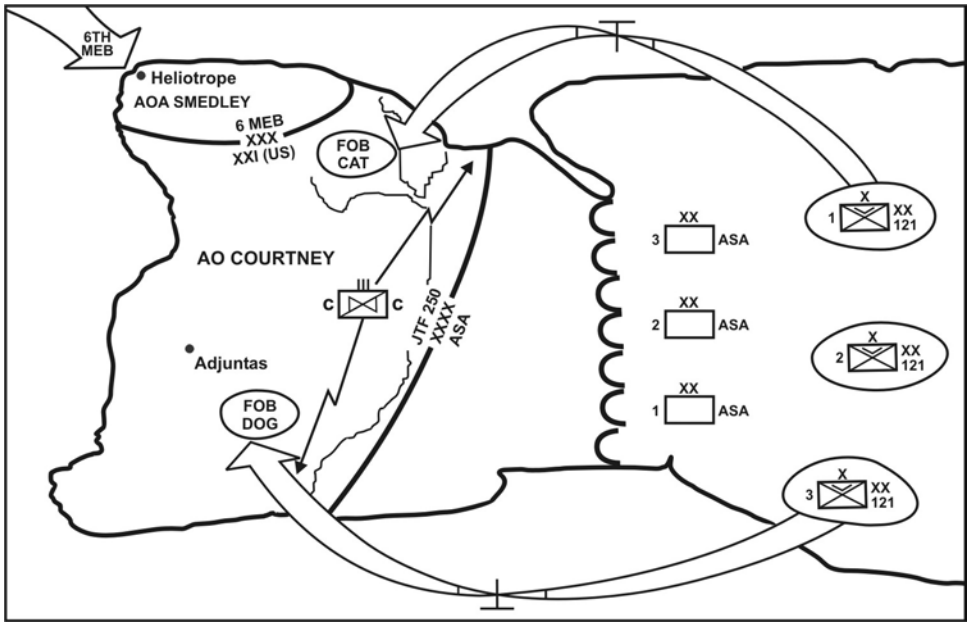
Figure B-17. COA and COA Sketch for Phase I of XXI Corps COA #1

1st Bn, 19th PSYOP Grp. Influence civilians in AO COURTNEY to comply with Government of San Anglos stay-put policy.

TCF. TCF doubles as corps reserve (entails accepting risk).

Reserve. Occupy AA Jackson. Plan in priority: (1) Commitment to block movement of additional Tiger Corps forces into AO COURTNEY; (2) support to civil authorities per OPLAN Provider; (3) counter Level III threats in JRA.

IO. TBD.



Sustaining. [omitted]

End state. (Phase I)

All Rendovan forces either destroyed or captured. XXI Corps and ASA units link up vicinity AWASH River. XXI Corps and 6th MEB link up vicinity of Heliotrope. XXI Corps transitions to support of San Anglos civil authorities and prepares to turn AO COURTNEY and AOA SMEDLEY over to ASA.

Figure B-17. COA and COA Sketch for Phase I of XXI Corps COA #1 (continued)

B-32. The following figures illustrate IO products needed to support one COA. Time permitting, the G-7 develops similar products to support each COA the staff develops. The G-7 develops the following IO products:

- IO concept of support.
- IO objectives and IO tasks to support each IO objective.
- IO input work sheets.
- IO synchronization matrix.
- IO-related target nominations (HPTs).
- Critical asset list

- Assessment of IO-associated risk.
- Criteria of success and IO IRs to support IO assessment.

Information Operations Concept of Support

B-33. While the staff is developing COAs, the G-7 develops an IO concept of support (based on the initial IO mission statement) for each one (see figure B-18). The G-7 has identified two offensive IO objectives that are added to the defensive IO objectives identified during mission analysis.

IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 systems and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans. IO objectives, in priority, are—

1. Prevent compromise of XXI Corps mission and concept of operations.

2. Protect XXI Corps C2.

3. Disrupt 109th Division ADA, ISR, C2, and targeting systems during critical periods of the operation.

4. Minimize civilian interference in objective areas.

Figure B-18. IO Concept of Support and IO Objectives for XXI Corps COA #1

Information Operations Objectives and Information Operations Tasks

B-34. The G-7 identifies and refines IO objectives and IO tasks as concepts of operations are developed for each COA. The XXI Corps G-7 elects to use IO input work sheets to prepare for COA analysis.

Information Operations Input Work Sheets

B-35. The G-7 staff prepares one IO input work sheet for each IO objective in each IO concept of support. Figures B-19–B-22, pages B-25–B-32, show work sheets prepared the IO objectives supporting COA #1. Because echelons above corps conduct CNO, CNA, and CNE, figures B-19–B-22 do not show these three IO elements.

Information Operations Synchronization Matrix

B-36. The IO synchronization matrix shows the execution time and duration of all IO tasks (see figure B-23, page B-33). It also shows which IO objective each IO task supports. To synchronize IO with the overall operation, the matrix shows major events for each battlefield operating system. It may serve as the IO concept of support sketch. The IO synchronization matrix for the approved COA becomes the basis for the IO execution matrix for the operation.

COA # 1	XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.					
IO Concept of Support	IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans.					
IO Objective #1	Prevent compromise of the XXI Corps mission and concept of operations					
	EW	**PSYOP**	**Military Deception**	**Physical Destruction**	**OPSEC**	**IA**
What (Task)	**Task EW-01** Disrupt Rendovan communications interception and locating systems	**Task PSY-01** Minimize resistance and interference of locals in AO Courtney	**Task MD-01** Deceive the Tiger Corps cdr as to the XXI Corps mission	**Task PD-01** Degrade Rendovan ISR systems in the Tiger Corps	**Task OP-01** Deny Tiger Corps knowledge of JTF mission	**Task IA-01** Protect XXI Corps and 121st ID INFOSYS and C2 systems
Why (Purpose)	To prevent collection of EEFI and location of friendly CPs	To prevent compromise of corps mission by civilian interference	To protect the air assault force from ADA fires and ground counterattack	To disrupt intelligence collection and C2	To prevent detection and location of critical air assault assets and support deception story	To provide RI to cdrs throughout the operation
Who	21st MI Bde 121st ID MI Bn	XXI Corps PSYOP Support Element	21st MI Bde	Corps and division artillery systems, attack helicopters, AI	System operators. CI personnel. A/322nd MI Bn (ACE)	All XXI Corps and 121st ID units
Where	Tiger Corps communications intercept and locating systems	AO Courtney	HQ Tiger Corps	Tiger Corps ISR systems	Throughout AO	Throughout AO
When	H – 1	H – 24	Ongoing	H – 5	Ongoing	Ongoing
Counteraction	Attack of friendly EA assets	Propaganda by Rendovan government	Increased ISR collection operations	Move ISR systems	Increased ISR collection operations	Rendovan forces increase CNA and EW attacks
Criteria of Success	Interruption of targeted systems Confirmation from ISR that targeted systems not working	Noninterference by local population	Movement of Rendovan forces to where they cannot affect the operation	BDA from observed fires	Achieving surprise for air assault	Commanders receive RI throughout the operation
IO IR	XXI Corps systems not detected	Movement of civilians	Movement of targeted units	CI not detecting collection	Counterreconnaissance operations reports	Rendovan capabilities and intentions to attack INFOSYS/ C2 systems
Remarks	XXI Corps approves	JTF 250 approves	JTF 250 approves	XXI Corps approves	Each HQ approves	Each HQ approves

Figure B-19. IO Input Work Sheet, IO Objective #1

COA # 1	XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.						
IO Concept of Support	IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans.						
IO Objective #1	Prevent compromise of XXI Corps mission and concept of operations						
	Counter-propaganda	**Counter-deception**	**Physical Security**	**CND**	**CI**	**PA**	**CMO**
What (Task)		**Task CD-01** Exploit Rendovan deception plan	**Task PS-01** Protect XXI Corps INFOSYS from sabotage	**Task CND-01** Protect XXI Corps INFOSYS against CNA	**Task CI-01** Assess OPSEC program	**Task PA-01** Assess effects of media coverage on PSYOP	**Task CMO-01** Support PSOP with feedback on PSYOP theme
Why (Purpose)		Ensure Rendovan deception operations do not deceive friendly cdrs	To counter Rendovan sabotage attempts	To prevent hostile collection from friendly INFOSYS	To counter Rendovan HUMINT, SIGINT, and IMINT	To determine if corps' mission appears in media	To input to possible compromise
Who		21st MI Bde	All units	All G-6/S-6 IANM, IASO, SA in all units	21st MI Bde	XXI Corps PAO	365 CA Bde
Where		Tiger corps C2 system	Throughout AO	Throughout AO	Throughout AO	Throughout AO	Throughout AO
When		Ongoing	Ongoing	Ongoing	Ongoing	Ongoing	Ongoing
Counteraction		Rendovan forces modify or cease deception operation	Rendovan forces change their sabotage methods	Rendovan forces reinforce CNA	Rendovan forces change their espionage and sabotage methods	None	None
Criteria of Success		Rendovan deception operations identified and countered	No evidence of sabotage	Rendovan CNA does not affect XXI Corps computers	No evidence that operation is compromised	CI shows no compromise	PSYOP themes are working
IO IR		Identify the Rendovan deception story	Indicators of sabotage	Indicators of Rendovan CNA	Indicators of Rendovan espionage and sabotage	Indicators of PSYOP message working	Indicators Tiger Corps knows corps mission
Remarks		JTF 250 approves	XXI Corps approves	STRATCOM approves	JTF 250 approves	JTF 250 approves	TF 250 approves

Figure B-19. IO Input Work Sheet, IO Objective #1 (continued)

COA # 1	XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.					
IO Concept of Support	IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans.					
IO Objective #2	Protect XXI Corps C2					
	EW	**PSYOP**	**Military Deception**	**Physical Destruction**	**OPSEC**	**IA**
What (Task)	**Task EW-02** EP protects XXI Corps personnel and equipment	**Task PSY-02** Enhance the IA in mind of Tiger Corps cdr	**Task MD-02** Cause Tiger Corps to believe CND of JTF is greater than it is		**Task OP-02** Deny Tiger Corps knowledge of XXI Corps mission	**Task IA-02** Protect XXI Corps INFOSYS and C2 system
Why (Purpose)	To ensure lack of interference of operations	To portray a greater IA capability than the XXI corps processes	To portray a greater CND capability than the XXI Corps processes		Prevent detection and location of critical air assault assets Support deception story	Provide RI to cdrs throughout the operation
Who	21st MI Bde	1st Bn, 19th PSYOP Grp and corps G-6	1st Bn, 19th PSYOP Grp and corps G-6		INFOSYS operators, CI personnel, HQ 121st ID	All XXI Corps units
Where	Throughout AO	HQ Tiger Corps	HQ Tiger Corps		Throughout AO	XXI Corps, 121st ID HQ and C2 nodes
When	H – 24	H – 48	H – 48		Ongoing	Ongoing
Counteraction	Increased EA by Rendovan forces	Increased CNA/EA by Rendovan forces	Increased CNA by Rendovan forces		Increased ISR collection operations	Rendovan forces increase CNA and EW attacks
Criteria of Success	EP not degraded	IA not changed	CND not changed		Achieving surprise for air assault	Cdr receives RI throughout the operation
IO IR	Rendovan EA capabilities	Indications of Rendovan CNA and EA	Indications of Rendovan CNA.		Counterreconnaissance operation reports	Rendovan capabilities and intentions to attack INFOSYS/C2 system
Remarks	JTF 250 approves	JTF 250 approves	STRATCOM approves		Each HQ approves	Each HQ approves

Figure B-20. IO Input Work Sheet, IO Objective #2

COA # 1	XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.						
IO Concept of Support	IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans.						
IO Objective #2	Protect XXI Corps C2.						
	Counter-propaganda	**Counter-deception**	**Physical Security**	**CND**	**CI**	**PA**	**CMO**
What (Task)	**Task CP-01** Provide EA targets and emphasize EP	**Task CD-01** Exploit Rendovan deception plan	**Task PS-02** Safeguard EW equipment	**Task CND 02** Protect XXI Corps INFOSYS against CNA	**Task CI-02** Assess OPSEC program	**Task PA-02** Protect soldiers against misinformation or disinformation	**Task CMO-02** Coordinate for HN support to counter enemy agents
Why (Purpose)	To protect corps C2	To ensure Rendovan deception operations do not deceive friendly cdrs	To protect corps C2	To ensure C2 is not disrupted	To counter Rendovan HUMINT, SIGINT, and IMINT	To enhance corps C2	To take advantage of ASA CI assets and familiarity with the AO
Who	1st Bn, 19th PSYOP Grp	21st MI Bde	XXI Corps, 121st ID G-6; Bde/Bn S-2s	All G-6/S-6 IANM, IASO, SA, in all units	21st MI Bde	XXI Corps PAO	365 CA Bde
Where	XXI Corps C2 nodes	AO Courtney	21st MI Bde	Throughout AO	All XXI Corps and 121st ID Units	Throughout AO	Throughout AO
When	Ongoing	Ongoing	Ongoing	Ongoing	Ongoing	Ongoing	Ongoing
Counteraction	Increased propaganda	Rendovan forces modify or cease deception operation	EW equipment penetrated	Rendovan forces reinforce CNA	Rendovans change collection methods	Rendovans increase misinformation	Rendovans use local sympathizers as agents
Criteria of Success	C2 systems protected by EP	Rendovan deception operations identified and countered	Lack of penetration	XXI Corps worldwide network and LAN are secure	No evidence of OPSEC lapses	No evidence of new misinformation	ASA supports XXI Corps CI efforts
IO IR	Lack of Rendovan EA	Identify the Rendovan deception story	Identify Rendovan attempts to penetrate	Indicators of Rendovan CNA	Indications of Rendovan collection efforts	Indicators of increased misinformation	Indicators of lack of support
Remarks	XXI Corps approves	JTF 250 approves	XXI Corps approves	STRATCOM approves	XXI Corps approves	XXI Corps approves	STRATCOM approves

Figure B-20. IO Input Work Sheet, IO Objective #2 (continued)

COA # 1	XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.					
IO Concept of Support	IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans.					
IO Objective #3	Disrupt 109th Division ADA, ISR, C2, and targeting systems during critical periods of the operation					
	EW	**PSYOP**	**Military Deception**	**Physical Destruction**	**OPSEC**	**IA**
What (Task)	**Task EW-03** Disrupt 109th ID ADA C2 **Task EW-04** Conduct nonlethal SEAD	**Task PSY-03** Broadcast PSYOP products over Tiger Corps C2 frequency	**Task MD-03** Cause 109 ID units to defend C2 system that XXI corps does not plan to destroy	**Task PD-02** Destroy ADA target identification, processing and firing systems **Task PD-03** Destroy ADA CPs	**Task OP-03** Conceal physical and electronic INFOSYS locations	**Task IA-03** Assure links between HQ XXI Corps and JTF 250
Why (Purpose)	To protect the air assault forces from ADA fires	To disrupt C2 frequencies	To divert 109th ID resources from other areas	To protect the air assault force from ADA fires	Ensure fire control and C2 links are operating	Ensure fire control and C2 links are operating
Who	Commander Solo 21st MI Bde	1st Bn, 19 PSYOP Grp	XXI Corps G-3	XXI Corps Artillery	Corps/div G-3s; Bde/Bn S-3s	Corps G-6
Where	Current locations of 109th ID ADA C2 nodes	Current locations of Tiger Corps ADA C2 nodes	Current locations of 109th ID C2 nodes	Current locations of Rendovan ADA units	XXI Corps and 121st ID INFOSYS nodes	HQ XXI Corps and HQ JTF 250
When	H – 1	H – 24	H – 48	H – 1	Ongoing	Ongoing
Counteraction	Reprogram EA/EP systems	Reprogram C2 systems	Resources diverted	ADA units relocate or reconstitute	Increased 109th ID ISR attempts	None
Criteria of Success	Lack of ADA fires Confused transmissions	Disruption of C2 frequencies	Increased defense activities	Lack of signals from targeted systems	Locations not compromised	Links intact
IO IR	Changes in Rendovan emitter parameters Jamming effectiveness reports	Changes in Rendovan emitter parameters	New units being defended	Specific locations of ISR and ADA assets Aerial BDA	Tiger Corps increases intelligence collection	Indications of penetrations
Remarks	XXI Corps approves	JTF 250 approves	XXI Corps approves	XXI Corps approves	XXI Corps approves	JTF 250 approves

Figure B-21. IO Input Work Sheet, IO Objective #3

COA # 1	XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.						
IO Concept of Support	IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans.						
IO Objective #3	Disrupt 109th Division ADA, ISR, C2, and targeting systems during critical periods of the operation						
	Counter-propaganda	**Counter-deception**	**Physical Security**	**CND**	**CI**	**PA**	**CMO**
What (Task)		**Task CD-02** Identify targets in the Tiger Corps deception plan	**Task PS-03** Safeguard EW equipment	**Task CND-03** Protect fire control systems of XXI Corps Artillery		**Task PA-03** Assess effects of media coverage of PSYOP broadcasts	
Why (Purpose)		To target 109th ID ADA, ISR, C2 systems	To allow EA against 109th ID ADA, ISR and C2 systems	To allow EA against 109tj ID ADA, ISR and C2 systems		To determine if disruption is effective	
Who		XXI Corps and 121st ID G-2s	21st MI Bde	XXI Corps G-6		XXI Corps PAO	
Where		109th ID ADA, ISR and C2 nodes	HQ 21st MI Bde	HQ, XXI Corps Artillery		International media coverage	
When		H – 48	Ongoing	Ongoing		Ongoing	
Counteraction		None, if successful	None	Increased CNA		Rendova uses media to disseminate counter-PSYOP	
Criteria of Success		ADA, ISR, C2 targets are found	EW equipment secure	Fire control systems remain operational		Media coverage favorable to JTF 250	
IO IR		Locations of 109th ADA, ISR, C2 nodes	None	Locations of 109th ID ADA, ISR, C2 nodes		Locations of 109th ID ADA	
Remarks		XXI Corps approves	XXI Corps approves	STRATCOM approves		JTF 250 approves	

Figure B-21. IO Input Work Sheet, IO Objective #3 (continued)

COA # 1	XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.					
IO Concept of Support	IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans.					
IO Objective #4	Minimize civilian interference in the objective area					
	EW	**PSYOP**	**Military Deception**	**Physical Destruction**	**OPSEC**	**IA**
What (Task)	**Task EW-05** Conduct EA to reduce Tiger Corps' access to electromagnetic spectrum	**Task PSY-04** Influence locals to comply with the stay-put policy	**Task MD-04** Provide information compatible with stay-put theme		**Task OP-04** Conceal XXI Corps' true mission	**Task IA-04** Ensure links between XXI Corps and JTF 250 are intact
Why (Purpose)	To reduce Rendovan messages to locals	To prevent civilian interference with the operation and minimize civilian casualties	To prevent civilian interference with the operation and minimize civilian casualties		To prevent civilian interference with the operation and minimize civilian casualties	To prevent civilian interference with the operation and minimize civilian casualties
Who	21st MI Bde	JTF aircraft-EA6b 1st Bn, 19th PSYOP Grp, 121st ID PSYOP Tm	1st Bn, 19th PSYOP Grp		XXI Corps and 121st ID units	XXI Corps G-6, JTF 250 J-6
Where	AO Courtney	AO Courtney	AO Courtney		Throughout AO	HQ XXI Corps, HQ JTF 250
When	H – 48	H – 48	H – 48		H – 48	H – 48
Counteraction	Increase EP	Counter misinformation campaign	Increase displaced persons		Penetrate OPSEC	Penetrate communications links
Criteria of Success	Messages to locals significantly reduced	Minimal civilian presence in objective areas	Minimal civilian presence in objective areas		XXI Corps mission not compromised	Minimal civilian presence objective areas
IO IR	Are there reduced messages to civilians?	Location of large concentrations of DCs. Needs and intentions of DCs	Location of large concentrations of DCs. Needs and intentions of displaced		Indication of OPSEC penetration	Links are not broken
Remarks	XXI corps approves	Combatant cdr approves	JTF 250 approves		XXI Corps approves	JTF 250 approves

Figure B-22. IO Input Work Sheet, IO Objective #4

COA # 1	XXI Corps conducts a one-division air assault, D-day, H-hour, over two aerial axes of advance to seize Objectives DOG and CAT. 27th ACR covers corps east flank and links up with ASA forces advancing westward. Division clears AO COURTNEY and links up with 6th MEB.						
IO Concept of Support	IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference within AO COURTNEY through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans.						
IO Objective #4	Minimize civilian interference in the objective area						
	Counter-propaganda	**Counter-deception**	**Physical Security**	**CND**	**CI**	**PA**	**CMO**
What (Task)	**Task CP-03** Degrade Rendovan disinformation		**Task PS-04** Safeguard San Anglos leadership	**Task CND-04** Prevent PSYOP message compromise	**Task CI-04** Counter Rendovan HUMINT	**Task PA-04** Influence civilian populace to support US objectives	**Task CMO-03** Influence DCs to stay put
Why (Purpose)	Prevent DC movement into objective areas		Prevent DC movement into objective areas	Prevent DC movement into objective areas	Prevent DC movement into objective areas	Prevent DC movement into objective areas	Prevent civilian interference in objective areas
Who	1st Bn, 19th PSYOP Bde, 121st ID PSYOP Tm		JTF 250 CMO	XXI Corps G-6	21st MI Bde	JTF and corps PAOs	365 CA Bde
Where	Throughout AO		San Anglos	HQ 1st Bn, 19th PSYOP Grp; HQ 121 ID PSYOP Tm	Throughout AO	Corps media operations center and designated unit locations	Throughout AO
When	Ongoing		Ongoing	Ongoing	Ongoing	Ongoing	Ongoing
Counteraction	Rendovan forces increase propaganda efforts or changes story		San Anglos leadership causes interference	Rendova increases CNA	Rendovan increases HUMINT	Rendovan forces increase propaganda	Rendovan attacks against HN assets Rendovan propaganda for people to move
Criteria of Success	DCs do not move into objective areas		DCs do not interfere with operation	DCs do not move into objective areas	DCs do not move into objective areas	Enhanced international and local support for JTF 250 operations	No attacks against critical assets Minimum Interference from DCs
IO IR	Location of large DC concentrations DC needs and intentions		Location of large concentrations of DCs	Indicators of compromise	Location of Rendovan HUMINT sources	Tenor and focus of press coverage of the operation	Locations of large concentrations of DCs Needs and intentions of DCs.
Remarks	JTF 250 approves		JTF 250 approves	STRATCOM approves	XXI corps approves	JTF 250 approves	JTF 250 approves

Figure B-22. IO Input Work Sheet, IO Objective #4 (continued)

H – 48	H – 24	H – 5	H – 1	D-Day H-hour	H + 24	H + 48	IO Objectives
PA-01 CMO-01 CI-01 OP-01 CD-01 PS-01 CND-01 IA-01 MD-01	PSY-01 →	PD-01 →	EW-01 →			→	**IO OBJ #1** Prevent compromise of XXI Corps mission and concept of operations
PSY-02 MD-02 CND-02 CI-02 PA-02 CMO-02 CD-01 IA-02 CP-01 PS-02 OP-02	EW-02 →					→	**IO OBJ # 2** Protect Corps C2
MD-03 CD-02 PA-03 OP-03 IA-03 PS-03 CND-03	PSY-03 →		EW-03 EW-04 →			→ →	**IO OBJ #3** Disrupt 109 ADA, ISR, C2 Systems
			PD-02 PD-03 →			→	
EW-05 PSY-04 MD-04 OP-04 IA-04 CP-03 CMO-03 PA-04 CI-04 PS-04 CND-04						→	**IO OBJ #4** Minimize Civilian interference
	DP to launch 121st ID			121 ID air assault	122 ID air movement		**Maneuver**
				Execute RFL PL Blue is boundary	PL Gray becomes LD		**C2**
Locate/track adversaries East of PL Blue				Track adversaries east of PL Blue	Track adversaries west of PL Blue		**Intelligence**
		SEAD		SEAD	SEAD		**Fire support**
	Wpns Hold			Wpns Tight	Wpns Tight		**Air defense**
				Priority to survivability in objective areas			**MCS**
						Jump BSAs to objective areas	**CSS**

Figure B-23. IO Synchronization Matrix

Information-Operations-Related Target Nominations

B-37. Based on IPB products, the high-value target, and information derived during mission analysis, the G-7 develops the EW and physical destruction IO tasks in figures B-19–B-22, pages B-25–B-32, into one or more IO-related targets. The G-7 nominates them as high-payoff targets (HPTs), as part of the targeting process. The targeting team determines which of these nominated targets are included in the high-payoff target list. (See appendix E.) The G-7 develops these IO-related HPTs and IO IRs needed to assess their effects as IO tasks and includes them on IO input work sheets and the IO assessment matrix (see figure B-26, page B-39).

Critical Asset List

B-38. The G-7 determines that there are no changes to the critical asset list developed during mission analysis (see figure B-6, page B-11) for COA #1. Critical assets may be added or deleted from the list based on how their loss or degradation would affect a COA.

Assessment of Information-Operations-Associated Risk

B-39. The staff assesses hazards associated with each COA as it is developed (see paragraphs B-16–B-18 and FM 100-14). The G-7 reviews each COA to determine tactical and accident hazards that may result from IO activities. The G-7 then develops controls to manage IO-related hazards, determines residual risk, and prepares to test the controls during COA analysis. The G-7 coordinates controls with other staff sections as necessary. Controls that require IO tasks to implement are added to the IO input matrix for the COA.

Mission: XXI Corps attacks D-day, H-hour to clear AO COURTNEY, link up with ASA forces vicinity AWASH River, and link up with 6th MEB vicinity HELIOTROPE; supports Government of San Anglos authorities in establishing order and providing basic services.

1 IO Objective	2 Identify Hazards	3 Assess Hazards	4 Develop Controls	5 Determine Residual Risk	6 Implement Controls
Disrupt Tiger Corps ADA, ISR, C2, and targeting during critical periods of the operation	Electronic fratricide	low	XXI Corps SOP	Low	XXI Corps SOP
Minimize civilian interference in the objective area	Large numbers of DCs generated by Rendovan operations may interfere with XXI Corps operations	extremely high	Early initiation of CMO/PSYOP actions to control interference may reduce the number of DCs in the objective area	Moderate	IO Annex

Figure B-24. IO Input to Risk Assessment (extract)

B-40. Figure B-24 shows the results of the G-7 risk analysis for the two offensive IO objectives developed for COA #1. The G-7 used the following logic during the risk analysis:

- **Initial assessment**.
  - **Electronic fratricide**. Disrupting the Tiger Corps and 109th Division ADA, ISR, C2, and targeting systems during critical periods of the operation risks electronic fratricide. However, the 21st MI Brigade is experienced in conducting EW and has worked frequently the JFACC and NAVFOR EW elements. XXI Corps units also have well-rehearsed SOPs for dealing with jamming and other electronic disruptions. The G-7, in consultation with the G-6, rates the severity of a hazard incident as marginal and the likelihood as seldom. Based on the risk assessment matrix at figure B-11, page B-15, the G-7 determines the risk associated with this task to be low.
  - **Civilian interference**. In consultation with the G-3, the G-7 determines that civilian interference in the objective area could result in mission failure (a catastrophic effect). According to the G-2, the probability that it will occur is likely unless the commander establishes some controls. Based on the risk assessment matrix at figure B-11, page B-15, the G-7 determines the risk associated with this hazard to be extremely high.
- **Residual risk**.
  - **Electronic fratricide**. Because the risk of **electronic fratricide** is low, G-2, G-3, G-6, and G-7 determine that no controls other than those mandated by SOP are necessary.
  - **Civilian interference**. The G-7 estimates that the CMO and PSYOP actions being planned will reduce the likelihood of civilian interference in the objective area from occasional to seldom. Based on the risk assessment matrix at figure B-11, page B-15, the G-7 determines the risk associated with it is moderate.

B-41. The G-7 lists the MDMP products or references that contain the controls in Column 6 of the risk assessment matrix. The G-7 then submits it to the G-3 for incorporation into the command risk management matrix.

Criteria of Success and Assessment

B-42. The IO criteria of success for each IO task are stated on the IO input work sheets (see figures B-19–B-22, pages B-25–B-24), and the IO assessment matrix (see figure B-26, page B-39).

RECOMMEND HEADQUARTERS

B-43. During this task, the G-7 identifies units to perform IO tasks and makes task-organization recommendations based on IO factors. The IO input worksheets show this information.

PREPARE COA STATEMENTS AND SKETCHES

B-44. The G-3 prepares a COA statement and supporting sketch for each COA for the overall operation (see figure B-17, page B-22).

MDMP TASK 4—COURSE OF ACTION ANALYSIS (WAR-GAMING)

B-45. As each COA is war-gamed, the G-7 confirms that the IO concept of support achieves what the commander intends and determines when to execute each IO task. The G-7 alters IO objectives and IO tasks if necessary

to synchronize them with the overall operation. The G-7 uses the IO input work sheets and the IO COA statements and sketches/synchronization matrixes as aids during COA analysis. The G-7 records the results of each war game, using either the synchronization matrix method or the sketch note method (see FM 5-0). The COA analysis product for IO is a refined IO concept of support for each COA, an execution time and duration for each IO task, and a list of advantages and disadvantages of each COA from the IO perspective.

MDMP TASK 5—COURSE OF ACTION COMPARISON

B-46. During COA comparison, the staff identifies the COA with the highest probability of success against the most likely enemy COA and the most dangerous enemy COA. The G-7's input to this analysis becomes paragraph 4 of the IO estimate (see appendix C).

MDMP TASK 6—COURSE OF ACTION APPROVAL

B-47. When COA comparison is complete, the staff is prepared to recommend which COA the commander should select. The G-7's recommendation becomes paragraph 5 of the IO estimate. Time permitting, the staff presents its recommendation to the commander at a decision briefing. At the end of the decision briefing, the commander decides which COA to adopt. The commander then refines the commander's intent and issues additional planning guidance.

B-48. After receiving the commander's guidance, the G-7 revises the IO concept of support for the approved COA as necessary. The WARNO that the G-3 issues after the commander approves a COA includes the final IO concept of support (see figure B-25).

[heading omitted]

WARNING ORDER 21-03

References: JTF 250 OPORD 01, DTG; XXI Corps WARNO 21-01; XXI Corps WARNO 21-02, DTG

Time Zone Used Throughout the Order: Zulu

1. **SITUATION**.

    a. **Enemy**. No change.

    b. **Friendly**. No change.

    c. **Attachments and detachments**. No change.

2. **MISSION**. No change.

3. **EXECUTION**.

Figure B-25. Third XXI Corps Warning Order (extract)

a. **Concept of operations**. [omitted; see figure B-17, page B-22]

(1-6) [omitted]

(7) **Information Operations**.

(a) **IO Concept of Support**. IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference in and around the objective area through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 systems and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF 250 and XXI Corps deception plans.

(b) **IO Objectives**.

(i and ii) IO Objectives 1 and 2. No change.

(iii) IO Objective 3. Disrupt 109th ID ADA, ISR, C2, and targeting during critical periods of the operation.

(iv) IO Objective 4. Minimize civilian interference in objective areas.

b. **Tasks to maneuver units**.

(1) 121st ID. No change.

(2) 27th ACR. No change.

c. **Tasks to combat support units**.

(1) 21st CAB. No change.

(2) 21st MI Bde. No change.

(3) 365th CA Bde. On order, support San Anglos civil authorities in restoring basic services.

(4) Corps Artillery. DS 121st ID. On order DS one FA brigade to 27th ACR.

(5) 1st Bn, 19th PSYOP Grp. [omitted]

d. **Coordinating Instructions**.

(1) Initial CCIR. No change.

(2) OPSEC Planning Guidance.

(a) EEFI. No change.

(b) Provisional OPSEC measures. [omitted]

(3) Risk guidance. [omitted]

(4) Deception guidance. [omitted]

Figure B-25. Third XXI Corps Warning Order (extract) (continued)

(5) Submit plans to G-3 plans NLT DTG.

(6) Rehearsal at AA Jackson, DTG.

4. **SERVICE SUPPORT**. [omitted]

5. **COMMAND AND SIGNAL**. [omitted]

ACKNOWLEGE: [authentication omitted]

Figure B-25. Third XXI Corps Warning Order (extract) (continued)

MDMP TASK 7—ORDERS PRODUCTION

B-49. The G-7 uses the products developed during the MDMP to prepare input to the OPORD. A complex operation, such as the one in this example, requires a separate IO annex. (See example at appendix D.) The minimum input is paragraph 3a(7) of the OPORD. Paragraph 3a(7) follows the format of paragraph 3 of the IO annex. In a time-constrained environment, the G-7 may prepare the IO annex as an execution matrix.

EXECUTION AND ASSESSMENT

B-50. The G-7 may prepare an IO execution matrix as an appendix to the IO annex (see appendix D). Normally, the IO synchronization matrix for the approved COA becomes the basis for IO execution matrix for the operation.

B-51. Commanders, assisted by the staff, continuously assess the situation and the progress of the operation, and compare it with the commander's visualization. The G-7 is responsible for assessing the effects of IO and recommending changes to the commander, when appropriate. The G-7 may prepare an assessment matrix to help with this function during execution (see figure B-26).

IO Task	Tasked Unit or Equipment	Desired Effect	Associated Target Information	Task Execution Status	Criteria of Success	Adversary Response
Task CD-01 Exploit Rendovan deception plan	21st MI Bde	Ensure Rendovan deception operations do not deceive friendly commanders		GREEN	Rendovan deception operations identified and countered	Rendovans modify or cease their deception operation
Task CD-02 Identify targets in the Tiger Corps deception plan	XXI Corps and 121st ID G-2	To target 109th ID ADA, ISR, C2 systems		GREEN	ADA, ISR, C2 targets are found	Rendovan forces modify or cease deception operation
Task CI-01 Assess OPSEC program	21st MI Bde	Prevent compromise of the operation Counter Rendovan HUMINT, SIGINT, and IMINT		GREEN	No evidence of compromise of operation No evidence of OPSEC lapses	Rendovan forces change espionage and sabotage methods
Task CI-02 Assess OPSEC program	21st MI Bde	Counter Rendovan HUMINT, SIGINT, and IMINT		AMBER	No evidence of OPSEC lapses	Rendovans change intelligence collection methods
Task CI–04 Counter Rendovan HUMINT	21st MI Bde	Prevent DCs movement into objective areas		AMBER	DCs do not move into objective areas	Rendovan increases HUMINT
Task CMO-01 Support PSYOP with feedback on PSYOP theme	365th CA Bde	Input to possible compromise		GREEN	PSYOP themes are working	Corps mission is compromised
Task CMO-02 Coordinate for HN support to counter enemy agents	365th CA Bde	Take advantage of ASA CI assets and familiarity with the AO		GREEN	ASA supports XXI Corps CI efforts	Rendovan use local sympathizers as agents
Task CMO-03 Influence DCs to stay put	365th CA Bde	Prevent civilian interference in objective areas		AMBER	No attacks against critical assets Minimum interference from DCs	Rendovans attack HN assets Rendovans increase propaganda for people to move
Task CND-01 Protect XXI Corps INFOSYS against CNA	All G-6/S-6 IANM, IASO, SA, in all units	To prevent hostile collection from friendly INFOSYS		GREEN	Rendovan CNA does not affect friendly computers	Rendovans reinforce CNA
Task CND-03 Protect fire control systems of XXI Corps Artillery	XXI Corps G-6	Allow EA against 109th ID ADA, ISR and C2 systems		AMBER	109th ID ADA, ISR, C2 targets are found	Rendovan forces increase CNA

Figure B-26. IO Assessment Matrix

IO Task	Tasked Unit or Equipment	Desired Effect	Associated Target Information	Task Execution Status	Criteria of Success	Adversary Response
Task CND-04 Prevent compromise of PSYOP message before release	XXI Corps G-6	Prevent DC movement into objective areas		AMBER	DCs do not move into objective areas	Rendovan forces increase CNA
Task EW-01 Disrupt Rendovan communications interception and locating systems	21st MI Bde, 121st ID MI Bn	Prevent collection of EEFI and location of friendly CPs		GREEN	Interruption of targeted systems Confirmation from ISR that locating systems not working	Attack friendly EA assets
Task EW-02 EP protects XXI corps personnel and equipment	21st MI Bde	Ensure lack of interference of operations.		AMBER	EP not degraded	Increased EA by Rendovan forces
Task EW-03 Disrupt 109th ID ADA C2	Commander Solo, 21st MI Bde	Protect the air assault forces from ADA fires		GREEN	Lack of ADA fire from units Confused transmissions	Rendovans reprogram EA/EP systems
Task EW-04 Conduct nonlethal SEAD	JTF 250 EW aircraft 21st MI Bde	Protect the air assault forces from ADA fires		GREEN	Lack of ADA fire from units Confused transmissions	Rendovans reprogram EA/EP systems
Task EW- 05 Conduct EA to reduce Tiger Corps' access to electromagnetic spectrum	21st MI Bde	Reduce Rendovan messages to locals		AMBER	Messages to civilians significantly reduced	Increased EP
Task IA-01 Protect XXI Corps and 121st ID INFOSYS and C2 systems	All XXI Corps and 121 ID units	Provide RI to commanders throughout the operation		AMBER	Commanders receive RI throughout the operation	Rendovan forces increase CNA and EW attacks
Task IA-02 Protect XXI Corps INFOSYS and C2 systems	All XXI Corps units	Provide RI to commanders throughout the operation		GREEN	Cdrs receive RI throughout the operation	Rendovan forces increase CNA and EW attacks
Task IA-03 Ensure links between HQ XXI Corps and JTF	Corps G-6	Ensure fire control and C2 links are operating		GREEN	Links intact	Links broken. Penetrate communications links
Task MD-01 Deceive the Tiger Corps cdr as to the XXI Corps mission	21st MI Bde	Protect the air assault force from ADA fires and ground counterattack		GREEN	Movement of Rendovan forces to where they cannot affect the operation	Increased ISR collection operations

Figure B-26. IO Assessment Matrix (continued)

IO Task	Tasked Unit or Equipment	Desired Effect	Associated Target Information	Task Execution Status	Criteria of Success	Adversary Response
Task MD -02 Cause Tiger Corps to believe CND of JTF 250 is greater that it is	1st Bn. 19th PSYOP Grp and Corps G-6	Protect the air assault force from ADA fires		GREEN	CND not changed	Increase CNA by Rendovan forces
Task MD- 03 Cause 109th ID units to defend C2 system that XXI corps does not plan to destroy	XXI Corps G-3	Divert 109th ID resources from other areas		GREEN	Increased defensive activates	Resources diverted
Task MD- 04 Provide information compatible with spy-put theme	1st Bn, 19th PSYOP Grp	Prevent civilian interference with the operation and minimize civilian casualties		AMBER	Minimal civilian presence in objective areas	Counter misinformation campaign
Task OP-01 Deny Tiger Corps knowledge of JTF 250 mission	System operators. CI personnel, A/322nd MI Bn (ACE)	Prevent detection and location of critical air assault assets Support deception story		GREEN	Achieving surprise for air assault	Increased ISR collection operations
Task OP-02 Deny Tiger Corps knowledge of XXI Corps mission	INFOSYS operators, CI personnel, HQ 121st ID	Prevent detection and location of critical air assault assets Support deception story		AMBER	Achieving surprise for air assault	Increased ISR collection operations
Task OP-03 Conceal physical and electronic INFOSYS locations	XXI Corps, Div G-3; Bde/Bn S3s	Ensure fire control and C2 links are operating		GREEN	Locations not compromised	OPSEC compromised
Task OP-04 Conceal corps true mission	XXI Corps, 121st ID units	To prevent civilians interference with the operation and minimize civilian casualties		AMBER	Minimal civilian presence in objective areas	Penetrate OPSEC Move ISR systems
Task PD-01 Degrade Rendovan ISR systems in the Tiger Corps	Corps and division artillery systems, attack helicopters, AI	Disrupt intelligence collection and C2		AMBER	BDA from observed fires	Move ISR systems
Task PD-02 Destroy ADA target identification, processing systems, and firing systems in Tiger Corps	XXI Corps Artillery	Protect the air assault force from ADA fires		GREEN	Lack of signals from targeted systems	ADA units relocate or reconstitute

Figure B-26. IO Assessment Matrix (continued)

IO Task	Tasked Unit or Equipment	Desired Effect	Associated Target Information	Task Execution Status	Criteria of Success	Adversary Response
Task PSY-01 Minimize resistance and interference of locals in AO Courtney	XXI Corps PSYOP Support Element.	Prevent compromise of corps mission by civilian interference		AMBER	Noninterference by local population	Propaganda by Rendovan government
Task PSY-02 Enhance the IA in mind of Tiger Corps cdr	1st Bn. 19th PSYOP Grp and Corps G-6	To portray a greater IA capability than the XXI Corps processes		GREEN	IA not changed	Increase EA by Rendovan forces
Task PSY-03 Broadcast PSYOP products over Tiger Corps C2 frequency	1st Bn. 19th PSYOP Grp	To disrupt C2 frequencies		AMBER	Disruption of C2 frequencies	Reprogram C2 systems
Task PSY-04 Influence locals to comply with the stay-put policy	JTF aircraft EA6b. 1st Bn, 19th PSYOP Grp 121st ID PSYOP Tm	Prevent civilian interference with the operation and minimize civilian casualties		GREEN	Minimal civilian presence in objective areas	Rendovan counter-misinformation campaign
Task CP-01 Provide EA targets and emphasize EP	1st Bn, 19th PSYOP Grp	To protect corps C2		GREEN	C2 systems protected by EP	Increased propaganda
Task CP-02 Provide target locations for physical destruction	1st Bn, 19th PSYOP Grp	To target 109th ID ADA, ISR, C2 systems		GREEN	ADA, ISR, C2 targets are found	109th ID forces increases their OPSEC
Task CP-03 Degrade Rendovan disinformation	1st Bn, 19th PSYOP Bde 121st ID PSYOP Tm	Prevent DC movement into objective areas		AMBER	DCs do not move into objective areas	Rendovans increase propaganda efforts or changes story
Task PA-01 Assess effects of media coverage on PSYOP	XXI Corps PAO	To determine if corps mission appears in media		GREEN	CI shows no compromise	Tiger Corps sources know mission of corps Rendova increases misinformation
Task PA-03 Assess effects of media coverage of PSYOP broadcast	XXI Corps PAO	To determine if disruption is effective		GREEN	ADA, ISR, C2 targets are found	No media coverage
Task PA-04 Influence civilian populace to support US objectives	JTF and corps PAO	Prevent DC movement into objective areas		AMBER	Enhanced international and local support for JTF operations	Rendovans increase propaganda

Figure B-26. IO Assessment Matrix (continued)

Appendix C

Information Operations Estimate

The information operation (IO) estimate is the G-7's evaluation of how IO factors may influence courses of action the commander is considering. This appendix discusses the IO estimate. It addresses how the G-7 develops and maintains it, and its relationship to the tasks of the military decisionmaking process. It shows which paragraphs of the estimate contribute to the IO annex of operations plans and operations orders. It includes an annotated IO estimate format and an example of a completed IO estimate based on the scenario in appendix B.

INFORMATION OPERATIONS ESTIMATE DEVELOPMENT

C-1. The information operations (IO) estimate supports decisionmaking throughout an operation. It is particularly helpful during the military decisionmaking process (see figure C-1). The IO estimate shows how IO can best be integrated into the overall operation. An effective G-7 begins to compile

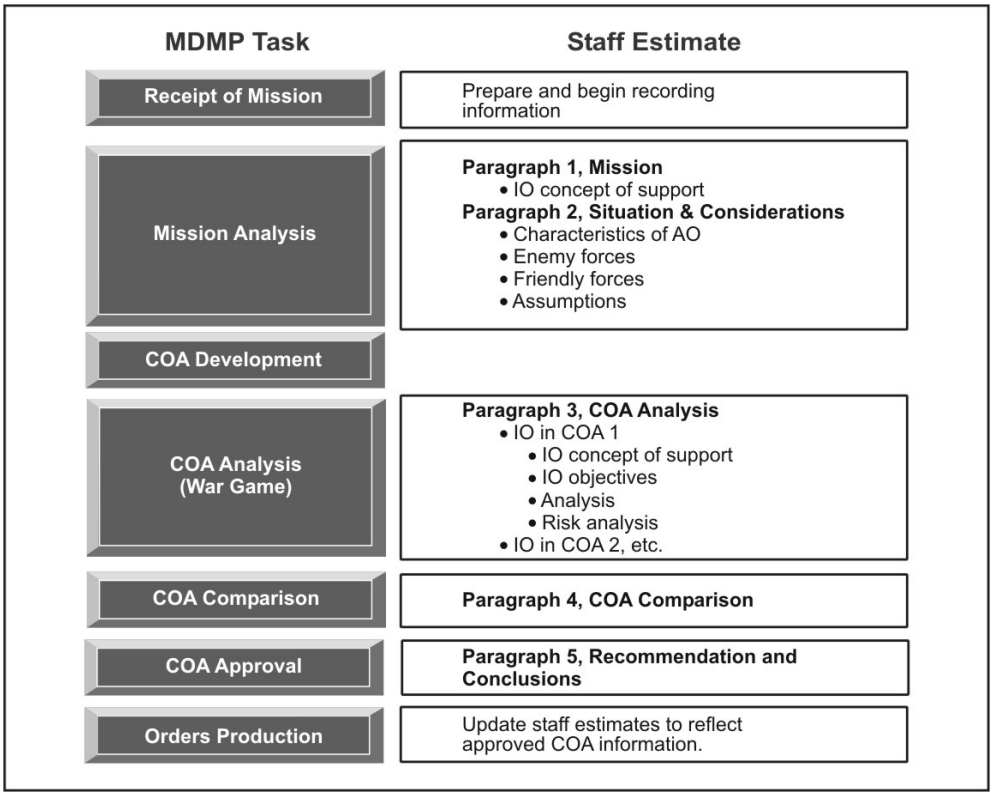


Figure C-1. IO Estimate Contributions to the MDMP

the IO estimate immediately upon receipt of the higher command's warning order, or sooner if possible.

C-2. The IO estimate and supporting estimates prepared for some IO elements are running estimates (see FM 6-0). They are living documents that are continuously updated throughout the operations process. This is a staff tool for assessing during preparation and execution.

C-3. Units below corps level rarely prepare written staff estimates. At those levels, a staff estimate usually consists of verbal summaries of available information backed up by overlays and charts. However, the staff estimate format is less an outline for a written product than it is a way to organize information. Maintaining a running IO estimate means that the G-7 maintains current information on all aspects of the situation and is prepared to make recommendations on decisions the commander must make. The IO estimate format lists aspects of the situation in a logical sequence. The G-7 may use it as a briefing aid to ensure that all aspects of the situation are addressed.

C-4. Normally the IO estimate provides enough information to complete the first draft of the IO annex and write the IO paragraph for the base operation order (OPORD) or operation plan (OPLAN). The estimate's depiction of the future also contributes to the commander's visualization. The estimate-derived initial IO annex should be enough to begin an operation. The IO estimate should be as comprehensive as possible within the time available.

C-5. Paragraphs 1 and 2 of the IO estimate are input to the mission analysis briefing. Paragraphs 3, 4, and 5 are input to the course of action (COA) decision briefing.

C-6. During peacetime, units maintain staff estimates for potential contingencies. These form the basis for staff estimates related to a specific mission. During operations, they maintain running estimates. These estimates address decision points, branches, and sequels. If no IO estimate exists, the G-7 begins developing one upon receipt of mission and refines it throughout the operation. Staff officers from IO elements provide input to the IO estimate. IO input to the OPLAN/OPORD comes from the IO estimate.

C-7. The focus of estimate development is on situation assessment rather than COA development. The purpose is not to develop a perfect plan, but to assemble information underlying an IO concept of support that can be modified to support overall concept of operations. Estimate development never stops. The IO estimate is continuously updated.

MISSION ANALYSIS

C-8. During mission analysis, the G-7 produces paragraphs 1 and 2 of the IO estimate. These paragraphs guide all subsequent IO planning—both for the current operation and for any branches and sequels. By the end of mission analysis, the IO estimate includes the following information—

- The restated IO mission (paragraph 1, the G-7 determines the initial IO mission during the analysis of the higher headquarters OPLAN/OPORD and the restated IO mission during mission analysis. At the same time the commander approves the restated mission for the overall operation, he approves the restated IO mission.)

- Characteristics of the area of operations (AO) and the information environment that may influence friendly and adversary operations (paragraph 2a, determined during IPB).
- Adversary IO-related capabilities in the AO (paragraph 2b, determined during IPB. It may be displayed as a situation template).
- Assets and resources that can be employed in an IO role (paragraphs 2c[2] and [3], determined during review of available assets).
- Critical IO facts and assumptions. (Facts are placed in the IO-estimate subparagraph [usually 2a, 2b, or 2c] that concerns them. Assumptions are placed in subparagraph 2e.)
- IO criteria of success for analyzing and comparing COAs (paragraph 2c(5).
- IO-related high-payoff target recommendations.
- IO information requirements.

C-9. At the end of mission analysis, paragraph 2 of the IO estimate is well formed. However, it is not complete. As part of a running estimate, it is updated as new information is received. Normally paragraph 2 of the IO estimate becomes the IO input to the mission analysis briefing.

COURSE OF ACTION COMPARISON

C-10. The G-7 uses the information in the IO estimate to refine IO objectives and check the soundness of the IO concept of support for each COA. The G-7 plans officer assesses the IO concept of support for each COA to ensure it can accomplish the IO objectives with available resources. The G-7 plans officer also assesses the general strengths and vulnerabilities of the IO concept of support for the COA. Special attention is paid to critical vulnerabilities that, if exploited by the adversary, could cause the IO to fail. The G-7 records the information gathered during COA development for use during COA analysis. The information developed during COA comparison and analysis forms the basis for paragraph three of the IO estimate.

C-11. During COA analysis, the G-7 confirms and refines the following information contained in the IO estimate:

- IO concept of support and IO objectives.
- IO strengths and vulnerabilities.
- IO resource requirements in terms of amount and effectiveness.
- IO effectiveness of risk control measures and resultant residual risk.

C-12. The assistant G-7 plans officer assesses the IO concept of support against the IO criteria of success, as each COA is war-gamed. The results of this assessment are the basis for the COA comparison recorded in paragraph four of the estimate.

RECOMMENDATIONS AND CONCLUSIONS

C-13. The G-7 staff analyzes the war-gaming of the IO concepts of support and compares the results for each COA with the others. The IO concepts of support are rank ordered according to how well they meet the evaluation criteria. Usually the comparison and ranking of the concepts of support are shown on a COA decision matrix. The matrix and a narrative explanation are recorded in paragraph four of the IO estimate.

C-14. After analyzing and comparing the IO concepts of support, The G-7 plans officer recommends the COA that the comparison shows IO can best support. The recommendation and summarized conclusions become the final paragraph of the IO estimate.

C-15. Once the commander approves a COA, the G-7 analyzes how each IO element can best support it. This is not a total reevaluation. Rather, the analysis done during COA comparison is explained based on the approved COA.

C-16. The G-7 prepares an IO estimate in the format shown in figure C-2.

G-7
Place of Issue
Date/Time Group

IO ESTIMATE NO. _____

References:
a. Maps and charts.
b. Other relevant documents.

1. **MISSION**. The restated IO mission from mission analysis.

2. **SITUATION AND CONSIDERATIONS**.

a. **Characteristics of the area of operations and information environment**. (Key IO factors from the intelligence estimate.)

(1) Weather. How different military aspects of weather will affect both friendly and adversary IO.

(2) Terrain and physical environment. How aspects of the terrain and the physical and environmental infrastructure will affect friendly and adversary IO.

(3) Information environment. Describe how the political, economic, sociological, psychological, and information environments will affect IO.

(4) Probable adversary picture of friendly forces.

b. **Enemy Forces**. Include key IO factors from the intelligence estimate. Address adversary dispositions, composition, capabilities, strength, and weaknesses likely to significantly affect COAs. Include the following subparagraphs. Add others as necessary.

(1) Decisionmakers and decisionmaking process.

(2) Information systems strength and vulnerabilities.

(3) IO capabilities, (including collection capabilities) disposition, composition, and strength.

(4) Likely IO COAs

c. **Friendly Forces**.

(1) IO concept of support for each COA.

Figure C-2. Annotated IO Estimate Outline

(2) Current status of IO assets.

(3) Current status of IO resources.

(4) Comparison of IO assets and resource requirements versus IO capabilities available and recommended solutions.

(5) Criteria of success to determine IO supportability for each COA:

(a) Measured against each of the IO effects.

(b) Cost versus benefits. Is accomplishing the effects worth the cost in resources and time?

(c) What are the chances of success for IO in each COA?

(6) Vulnerability assessment.

d. **Operations Security**.

(1) Essential elements of friendly information.

(2) OPSEC indicators. List by EEFI element and staff function.

(3) OPSEC measures in effect. List by EEFI element and staff function.

(4) OPSEC measures contemplated. List by EEFI element and staff function.

e. **Assumptions**. IO assumptions developed during mission analysis.

3. **COA ANALYSIS**. [For each friendly COA]

a. **COA 1**.

(1) Analyze the IO concept of support using the IO evaluation criteria and the war-gaming methodology (action-reaction-counteraction) to support the maneuver COA.

(2) Estimate the likelihood of accomplishing IO objectives in the available time, given friendly IO capabilities and vulnerabilities, versus those of the adversary.

(3) Determine the potential for unintended consequences of IO tasks and the possible impacts on both adversary and friendly COAs.

(4) Identify critical events that should be evaluated within COA analysis to assess defensive IO requirements.

(5) Assess the effectiveness of friendly and adversary IO-related capabilities in relation to each other, the effects of the AO as favorable or unfavorable to IO, and the most significant friendly and adversary IO-related vulnerabilities.

(6) Evaluate the risk of failure or compromise of IO in terms of effects on the success of the COA and the potential for loss or compromise of command assets.

(7) Analyze the risk in executing IO in the COA in terms of nonavailability or untimely availability of assessment.

Figure C-2. Annotated IO Estimate Outline (continued)

(8) List EEFI for this COA if different from paragraph 2d.

b. **COA 2**. [Repeat the process outlined above for all other COAs.]

4. **COA COMPARISON**. Compare the COAs in terms of the evaluation criteria. Rank-order COAs for each criterion. Visually support the comparison with a decision matrix.

a. Compare the costs of IO in each COA based on the resources and time required executing them in relation to the operational impact of their success.

b. Compare the levels of risk to COA success and friendly assets should IO fail or be compromised.

c. Summarize the advantages and disadvantages for IO in each COA to evaluate the chance of success in each.

5. **RECOMMENDATION AND CONCLUSIONS**.

a. Recommend a COA based on the comparison (most supportable from the IO perspective).

b. Present IO issues, deficiencies, risks, and recommendations to reduce their impacts.

/signed/

G-7

Appendix 1, OPSEC estimate, if used

Appendix 2, PSYOP estimate, if used

Figure C-2. Annotated IO Estimate Outline (continued)

C-17. Upon completion of the IO estimate, the G-7 will have prepared the majority of input needed for the OPLAN/OPORD. The G-7 can build most of the IO annex through "cut and paste" from a well-prepared IO estimate (see figure C-3).

STAFF ESTIMATE BRIEFING

C-18. The IO estimate may be presented as a briefing to provide IO information to the commander and staff. The briefing will normally elaborate on the key points derived from preparing the estimate, focusing principally on adversary and friendly IO capabilities and vulnerabilities, and support IO can provide to the COAs. The briefing is part of either the mission analysis briefing (paragraphs 1 and 2) or part of the commander's decision briefing (paragraphs 3, 4, 5). The briefing itself consists of all of paragraph one and a summary of paragraphs 2 through 5 of the IO estimate.

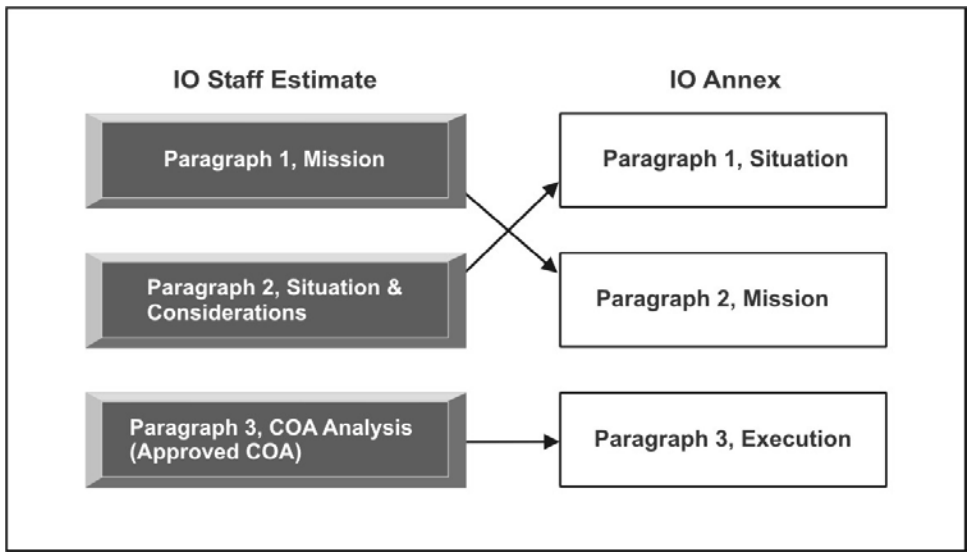


Figure C-3. IO Staff Estimate Contributions to IO Annex

SUMMARY

C-19. The IO estimate is both a process and a product. The process calls for a disciplined approach to collecting and processing information, and to recording the results. Automated tools such as databases and word processing programs give the G-7 the flexibility and responsiveness needed to tailor the estimate to meet a variety of requirements. The IO estimate is a living document that is continuously refined, as additional information becomes available. A current estimate allows the G-7 to quickly provide accurate information to meet planning requirements as they change.

Appendix D

Information Operations Annex

This appendix discusses the contents of the information operation (IO) annex to orders and plans. It includes annotated formats for an IO annex and its appendixes (see figures D-1–D-6, pages D-2–D-15), and examples of an IO annex (see figure D-7, pages D-15–D-19), and IO execution matrix (see figure D-8, page D-20).

INFORMATION OPERATIONS ANNEX DEVELOPMENT

D-1. The information operations (IO) annex serves three primary purposes:

- The situation paragraph provides operational details on the situation from an IO perspective.
- The execution paragraph and matrix provide the direction needed to focus the effects of the IO elements/related activities.
- The assessment matrix displays the information needed to assess IO tasks.

The IO annex also addresses service support, command, and signal aspects of IO that are not covered elsewhere in the operation plan (OPLAN)/operation order (OPORD). Some of the information in the IO annex is derived from the IO estimate. Major portions of the annex can be written directly from the IO estimate (see figure C-3, page C-7). Much of the information required for the execution and assessment matrices is taken from the IO input worksheets for the approved course of action (COA).

SITUATION PARAGRAPH

D-2. The situation paragraph provides operational details on the situation from an IO perspective. This description does not repeat the OPLAN/OPORD situation paragraph. It is tailored to aspects of the information environment that affect offensive and defensive IO. The situation paragraph describes how the information environment (including the civilian infrastructure) may affect friendly, adversary, and other force/group operations. It discusses how the information environment will influence protecting friendly critical assets.

EXECUTION PARAGRAPH AND MATRIX

D-3. The execution paragraph provides the direction needed to synchronize the effects of IO elements/related activities. It outlines the effects the commander wants IO to achieve. It describes the activities of the IO elements/related activities in enough detail to synchronize them.

D-4. The IO execution matrix is normally an appendix to the IO annex. It shows when each IO task is to be executed. The execution matrix helps the G-7

monitor and direct IO during execution. It also allows the G-7 to monitor the coordination needed to execute IO effectively without incurring unanticipated interference or information fratricide. Because they contribute significantly to massing combat power at a decisive point, the G-7 also places IO tasks in the G-3 execution matrix.

D-5. The IO execution matrix is not a tasking document. The G-7 places IO tasks under tasks to subordinate units in IO element appendixes or in the appropriate OPLAN/OPORD annex.

ASSESSMENT MATRIX

D-6. The G-7 incorporates the criteria of success for each IO task, the information required to measure task accomplishment, and the source of that information into the IO assessment matrix (see figure B-26, pages B-39–B-42). The IO input worksheets and IO synchronization matrix list this information, which was refined during the COA analysis.

D-7. The IO assessment matrix includes the IO information requirements (IRs) needed to produce IO-specific intelligence, identify high-payoff targets (HPTs), and assess IO task accomplishment. The G-7 crosswalks IO IRs with the collection plan.

Annex P (Information Operations) to OPORD No _____

1. SITUATION

a. Enemy.

(1) Terrain. List terrain aspects affecting each IO element.

(2) Weather. List weather aspects affecting each IO element.

(3) Enemy IO capabilities.

(a) Identify enemy IO elements.

(b) Identify enemy C2 vulnerabilities.

(c) Identify enemy capabilities to degrade friendly C2.

(d) Identify the enemy situation, force disposition, intelligence elements, and possible actions.

(e) Identify specific information that bears directly on the planned IO.

b. Friendly.

(1) Identify IO capabilities.

(2) Identify IO assets needed to attack enemy targets.

(3) Identify the friendly forces that will directly affect IO.

(4) Identify the critical limitations of planned IO.

Figure D-1. Annotated Information Operations Annex

(5) Identify potential conflicts within the friendly electromagnetic spectrum especially if conducting joint or multinational operations. Identify deconfliction methods and priority of spectrum distribution.

c. **Civil Considerations**. Identify other key people and groups of people in the AO.

d. Attachments and detachments.

(1) List IO assets that are attached or detached.

(2) List IO resources available from higher headquarters.

2. MISSION

State the IO mission statement.

3. EXECUTION

a. Scheme of Support.

(1) **Concept of Support**. Describe the IO concept of support and IO objectives. A complex IO concept of support may require a schematic to show IO objectives and IO task relationships. Include a discussion of the overall IO concept of support, with the specific details in element subparagraphs or appendixes. Refer to the execution matrix to clarify timing relationships among various IO tasks. This annex should contain the information needed to synchronize timing relationships of each of the elements/related IO activities. Include IO-related constraints, if appropriate.

(2) **Operations Security**. State how OPSEC tasks will deny the enemy knowledge of the EEFI. Synchronize this element with the other IO elements. Refer to appendix 1, Operations Security, for detailed information.

(3) **Psychological Operations**. State how the PSYOP tasks will degrade, disrupt, deny, or influence the enemy. Identify the audiences and desired effects, in priority, for PSYOP. Synchronize this element with the other IO elements. Refer to appendix 2, PSYOP, for detailed information.

(4) **Military Deception**. State how the MD tasks will deceive and influence the enemy. Synchronize this element with the other IO elements. Refer to appendix 3, Military Deception, for detailed information.

(5) **Electronic Warfare**. State how the EW tasks will degrade, disrupt, deny, and deceive the enemy. State the defensive and offensive EW measures. Identify target sets and effects, by priority, for EW operations. Synchronize this element with the other IO elements. Refer to appendix 4, Electronic Warfare, for detailed information.

(6) **Computer Network Operations**. For echelons above corps or a corps/division designated as a JTF, stating CNO requirements is appropriate. For a corps or lower echelon unit that is not designated as a JTF, CNO is not appropriate. In the case of a JTF, the CNO paragraph or appendix states CNO tasks in terms of CNA, CND, and CNE (as in the following paragraphs).

Figure D-1. Annotated Information Operations Annex (continued)

(7) **Computer Network Attack**. State how the CNA tasks will destroy, degrade, disrupt, and deny the enemy. Identify target sets and effect, by priority, for CNA. Synchronize this element with the other IO elements. Pass request for CNA to higher headquarters for approval and implementation.

(8) **Computer Network Defense**. State how CND will protect and defend computer networks. Synchronize this element with the other IO elements. Refer to annex H, Command, Control, Computer, and Communications, for detailed information.

(9) **Computer Network Exploitation**. For echelons above corps or a corps/division designated as a JTF, stating CNE requirements is appropriate. For a corps or lower echelon unit that is not designated as a JTF, CNE is not appropriate. In the case of a JTF, the CNE paragraph or appendix states the CNE tasks and synchronizes CNE with other IO elements. Pass requests for CNE to higher headquarters for approval and implementation.

(10) **Physical Destruction**. State how the physical destruction tasks will destroy, degrade, disrupt, and deny the enemy. Identify target sets and effects, by priority, for physical destruction. Synchronize this element with the other IO elements. Refer to annex D, Fire Support for detailed information.

(11) **Information Assurance**. State how the IA tasks will deny the enemy access to the friendly C2 system. Identify the information and INFOSYS for protection. Synchronize this element with the other IO elements. Refer to annex H, Command, Control, Computer, and Communications, for detailed information.

(12) **Physical Security**. State how the physical security tasks will deny the enemy. Synchronize this element with the other IO elements. Refer to annex K, Provost Marshal, for detailed information.

(13) **Counterintelligence**. State how the counterintelligence tasks will degrade, disrupt, deny, and exploit the enemy. Identify the units for protection. Synchronize this element with the other IO elements. Refer to annex B, Intelligence, for detailed counterintelligence information.

(14) **Counterdeception**. State how the counterdeception tasks will disrupt, deny, and exploit the enemy. Identify the units for protection. Synchronize this element with the other IO elements. Refer to annex B, Intelligence, for detailed counterdeception information.

(15) **Counterpropaganda**. State how the counterpropaganda objectives and counterpropaganda tasks will degrade, disrupt, deny, and exploit the enemy based on the approved COA. Identify the units for protection. Synchronize this element with the other IO elements. Refer to appendix 2, PSYOP for detailed counterpropaganda information.

(16) **Civil-Military Operations**. CMO is a related activity to IO. State how CMO supports the elements of IO. See annex U, Civil Military Operations, for detailed information.

Figure D-1. Annotated Information Operations Annex (continued)

(17) **Public Affairs**. PA is a related activity to IO. State the IO task for PA. See annex V, Public Affairs, for detailed information.

b. Tasks to Subordinate Units. Review specific and implied tasks by command.

(1) List IO tasks to maneuver units.

(2) List tasks to PSYOP units.

(3) List tasks to EW units.

(4) List IO tasks to counterintelligence units.

c. IO Cell.

(1). List members of the IO cell.

(2) State non-SOP tasks assigned to the IO cell.

d. Coordinating Instructions.

(1) Include only IO instructions common to two or more units not already covered in the base OPLAN/OPORD.

(2) State specific ROE for each IO element.

(3) Refer to IO appendixes for details.

(4) Do not include SOP information.

(5) List any constraints not contained in the concept of support.

4. SERVICE SUPPORT

Identify requirements for supply distribution, transportation, and HN support pertaining to IO as a whole. Service support to individual IO elements will be identified in their separate appendixes.

5. COMMAND AND SIGNAL

Significant command and signal information related to IO is normally covered in the body of the order. This paragraph covers arrangements needed to exchange information among IO elements.

Appendix 1, OPSEC

Appendix 2, PSYOP

Appendix 3, Military Deception

Appendix 4, Electronic Warfare

Appendix 5, IO Execution Matrix

Figure D-1. Annotated Information Operations Annex (continued)

Appendix 1 (OPSEC) to Annex P (Information Operations) to OPORD No _____

1. SITUATION

a. Enemy.

(1) Identify the estimated enemy's assessment of friendly operations, elements, and intentions.

(2) Identify the enemy's intelligence collection elements according to major categories (for example, SIGINT, HUMINT, and IMINT).

(3) Identify potential sources (including other nations) that provide support to the enemy.

(4) Identify unofficial intelligence organizations that support the national leadership, if any.

(5) Identify the enemy intelligence element strengths and weaknesses.

b. Friendly.

(1) State the EEFI of the higher headquarters.

(2) State the EEFI of the command.

(3) Identify the major OPSEC tasks.

c. Attachments and Detachments.

(1) Identify attachments required to conduct OPSEC.

(2) Identify detachments of units that enhance the OPSEC posture of the command.

2. MISSION

State how OPSEC will protect EEFI and support IO objectives.

3. EXECUTION

a. Scheme of Support.

(1) State the OPSEC tasks. Describe phased operations where applicable. Describe how OPSEC will help achieve the commander's intent and end state.

(2) List the OPSEC tasks not listed in the base OPORD and IO annex to be performed by maneuver elements. Ensure maneuver units implement the appropriate program against the current threat.

(3) List the countermeasures to be taken by the unit to ensure enemy collection efforts are unsuccessful.

(4) List countermeasures and counterintelligence methods, assets, and programs of special importance to operations. Include personnel security, physical security, COMSEC, SIGSEC, patrolling, and counterreconnaissance. Ensure efforts are aimed at both external and internal security threats.

Figure D-2. Annotated Operations Security Appendix

(5) State how OPSEC supports the other IO elements.

(6) Identify the concept for monitoring the effectiveness of OPSEC measures during execution.

(7) Identify the OPSEC-related IO IRs needed for feedback.

(8) Identify AAR requirements.

b. Tasks to subordinate units.

(1) List countermeasures that specific units are to implement.

(2) List the countermeasures that require special emphasis by assigned, attached, or supporting units. These countermeasures are designed to counter a specific enemy intelligence threat.

(3) Identify the specific OPSEC measures to be executed. List these by phase and include specific responsibilities for subordinate elements.

c. Coordinating Instructions.

(1) Identify OPSEC measures common to two or more units.

(2) Identify the required coordination with PA.

(3) Identify the guidance on termination of OPSEC-related activities.

(4) Identify the guidance on declassification and public release of OPSEC-related information.

4. SERVICE SUPPORT

Identify, if any, the OPSEC-related supply support requirements.

5. COMMAND AND SIGNAL

a. **Command**. State the location of the G-7.

b. **Signal**. Identify special or unusual OPSEC-related communications requirements, if any.

Figure D-2. Annotated Operations Security Appendix (continued)

Appendix 2 (PSYOP) to Annex P (Information Operations) to OPORD No._____

1. SITUATION

a. Enemy.

(1) State enemy resources and elements, both military and civilian, available to conduct PSYOP. State past enemy PSYOP efforts (who were targeted, using what means, and their effectiveness).

(2) Identify the enemy decisionmakers.

(3) Identify the characteristics of enemy decisionmakers, their key advisors, and staff (particularly intelligence analysts).

(4) Identify the enemy elements that affect counterpropaganda activities.

b. Friendly.

(1) Identify ongoing PSYOP programs, if any.

(2) Identify competing PSYOP goals in the AO.

(3) Identify PSYOP tasks to be accomplished.

(4) Identify the organizations that are not subordinate to this command and the counterpropaganda tasks assigned to each.

c. Attachments and Detachments.

(1) List PSYOP assets that are attached or detached.

(2) List PSYOP resources available from higher headquarters.

2. MISSION

State the PSYOP concept of support (who, what, where, how, when, why).

3. EXECUTION

a. Scheme of Support.

(1) State the PSYOP tasks.

(2) State the counterpropaganda concept of support.

(3) Identify the counterpropaganda activities occurring in each phase.

(4) Describe activity sequences in each phase, keyed to phase initiation and supported operational events. Identify the time-phased guidance for accomplishing actions implementing counterpropaganda.

b. Tasks to subordinate units.

(1) Ensure tasks clearly fix responsibilities and provide feedback on effectiveness of PSYOP activities.

Figure D-3. Annotated Psychological Operations Appendix

(2) Identify the command element responsible for coordinating counterpropaganda actions.

(3) Identify the counterpropaganda tasks assigned to each subordinate unit, to include identification of vulnerabilities.

c. Coordinating instructions.

(1) Identify activities and resources available to these neutral intentions.

(2) Identify neutral actions/behavior that favor mission accomplishment.

(3) Identify the characteristics of decisionmakers and their key advisors, major staff planners, staff factions (to include particularly influential individuals), and intelligence system analysts.

(4) Identify groups that can influence plans, decisions, and operational effectiveness in task accomplishment.

(5) Identify how susceptible these groups are to PSYOP.

(6) Identify the apparent goals, motivations, and characteristics of each group.

(7) Identify the leaders able to cause these groups to behave in various ways.

(8) Identify approved PSYOP objectives, themes to stress, and themes to avoid.

(9) Identify target audiences in the AO, to include key communicators. Identify relevant background information on target audience perspectives, vulnerabilities, effectiveness, and susceptibility to friendly and enemy PSYOP.

(10) Identify military activities and actions conducted by subordinate units that support or facilitate PSYOP efforts.

(11) Provide OPSEC guidance on PSYOP sensitivity and employment.

(12) State classification authority for PSYOP tasks.

(13) Address mechanisms for coordinating PSYOP with attached PSYOP support elements and assigned PSYOP staff.

(14) State procedures for coordinating fixed-wing, rotary-wing, UAV, and field artillery delivery of PSYOP products.

(15) State PSYOP-specific current intelligence requirements (or refer to the intelligence annex).

(16) State how intelligence, multidiscipline CI, security monitoring, and operational feedback will be provided.

(17) Identify coordination required with adjacent commands and civilian agencies.

Figure D-3. Annotated Psychological Operations Appendix (continued)

(18) Identify the detailed requirements for coordinating among elements involved in counterpropaganda.

(19) Identify, if any, the special security or handling requirements for counterpropaganda.

(20) Identify, if any, the operational reporting requirements necessary for effective monitoring of counterpropaganda tasks.

4. SERVICE SUPPORT

a. Identify resources required to conduct (plan, prepare, execute, and assess) PSYOP actions.

b. Identify logistic requirements. Include preparation, distribution, and stocking of PSYOP materials; transport of PSYOP material and personnel to operational areas, and their basing and support while conducting PSYOP; provisions for the supply and maintenance of US and indigenous PSYOP material; and fiscal and personnel matters.

c. Identify the provisions for control and maintenance of indigenous equipment and materials.

d. Identify the fiscal matters relating to special funds.

e. Identify the personnel matters relating to indigenous personnel.

5. COMMAND AND SIGNAL

a. Command.

(1) Identify how control will be effected and implementation centrally coordinated.

(2) Identify the recognition and identification instructions.

(3) Identify the headquarters locations and movements.

b. Signal.

(1) State the PSYOP approval and release authority that has been delegated or retained by higher headquarters.

(2) State the PSYOP approval authority the commander has delegated or specifically retained to subordinate commanders for the development of proposed PSYOP products, actions, and programs.

(3) State the PSYOP release authority the commander has delegated to subordinate commanders, or specifically retained, for releasing and disseminating approved PSYOP products in their respective AOs.

(4) Identify the INFOSYS that will be used to plan COAs and control, coordinate, and supervise execution of the approved COA.

(5) Identify the codeword.

Figure D-3. Annotated Psychological Operations Appendix (continued)

Appendix 3 (Military Deception) to Annex P (Information Operations) to OPORD No. ___

1. SITUATION

a. Enemy.

(1) Identify the assessed enemy goal or condition (favorable or unfavorable, as perceived through the enemy's perspective) that this deception plan is designed to counter or exploit.

(2) Identify significant enemy military capabilities that can affect the deception.

(3) Describe the deception target.

(4) Describe those biases and predispositions of the deception target.

(5) Discuss the ability of the deception target to respond to the deception. Discuss how the enemy has previously responded to similar events, conditions, and circumstances.

(6) Discuss probable enemy COAs and their possible results if deception is not used.

(7) Precisely identify the key conclusions, estimates, or assumptions that the deception target will have to accept as being true in order for him to act in accordance with the deception objective.

b. Friendly. Identify the deception plan of higher headquarters.

c. Attachments and Detachments.

(1) List units attached or detached in support of the deception.

(2) List assets that support the deception that are attached or detached.

(3) List resources available from higher headquarters to support the deception.

2. MISSION

State how the deception will support IO objectives.

3. EXECUTION

a. Scheme of Support.

(1) State the deception objective deception, target and deception story. Describe phased operations where applicable and describe how the deception plan will support achieving the commander's intent and end state.

(2) List the deception tasks not listed in the base IO annex to be performed by maneuver units. Ensure maneuver units implement the appropriate program against he current threat.

Figure D-4. Annotated Psychological Operations Appendix

(3) List the countermeasures to be taken by the unit to ensure enemy collection efforts are unsuccessful at exposing the deception operation.

(4) State how the deception supports the concept of operations. Describe how the deception is integrated into the IO annex. If applicable, list how the deception operation is phased.

(a) State other IO elements that will support the deception operation.

(b) State the other plans and operations pertinent to the deception.

(c) State the required coordination and deconfliction.

(5) Outline the framework for the deception operation and the deception means to be employed. A general description of the types of executions and means to be used to portray them will be identified for each operational phase. If applicable, include the time lines for major phase executions. Use tab A, Deception Event and Execution Schedule, to describe specific operations and events.

(6) State the intended effect of the deception on the deception target in terms of the specific action or inaction the deception operation is expected to elicit from the target. State exactly what we want the target to do or not to do with his forces, capabilities, or operations. Identify how friendly capabilities, the situation, conditions, or operations will be improved or protected if the target executes the desired actions.

(7) Outline the friendly actions that will be portrayed to cause the deception target to acquire the desired perceptions and appreciations. The deception story is presented in a style that replicates the style of the target. Identify what the target would expect to read in his own intelligence estimate.

b. Tasks to subordinate units.

(1) List deception tasks to subordinate units. Include in the task description the cover story, and a description of how the tasks support the overall deception plan. Include what enemy observation measures the tasks are intended to target.

(2) Specify execution and feedback tasking to elements participating in the execution and monitoring of the deception operation. Refer to tab C, Task Organization, if used.

c. Coordinating instructions.

(1) State the coordination of two or more units during specific deception tasks. State what data is to be collected on enemy forces to exhibit success or failure of the deception.

(a) Identify specific enemy intelligence operations and indicators that will be monitored to determine if deception executions are being sensed by hostile intelligence collection, analytic, or dissemination systems.

(b) Identify specific expected hostile actions or inactions that will indicate whether the deception target is acting per the deception objective.

Figure D-4. Annotated Psychological Operations Appendix (continued)

(2) Identify and rate as high, medium, or low the following risks: failure, compromise, and unintended effects.

(3) Discuss security measures and cover stories to be used in connection with the deception operations. Identify code words, nicknames, and special handling caveats and procedures for planning and executing documents, materials, and associated implementing activities. Refer to the OPSEC appendix.

(a) List specific security concerns, policies, practices, and procedures with general application to all participating personnel and associated activities.

(b) List specific security, concerns, policy, practices, and procedures that apply to specific persons, events, or activities.

4. SERVICE SUPPORT

a. Specify any special administrative measures that may be required for the execution of the deception operation.

(1) Identify general administrative requirements and procedures that apply to the execution of the deception operation.

(2) Identify any specific administrative tasks or procedures that should be highlighted to supporting administrative personnel and functions.

b. Provide an estimate of the expected material and resource expenditure of the deception plan.

5. COMMAND AND SIGNAL

a. Command. Specify the general and specific responsibilities of each echelon of command and headquarters for further deception implementation and execution activities.

(1) Approval Authority. Identify approval chain for the deception plan and the individual exercising plan approval authority.

(2) Oversight and Termination Authority. Identify the command echelon and commander responsible for monitoring the execution of the deception operation and the commander with routine authority to terminate the operation. Identify other individuals who may be authorized to terminate executions and operations in the event of extremely adverse or time-critical conditions.

b. Signal. Outline the communications means, methods, and signal operating instructions for control personnel and witting participants in the deception operations.

Tabs

Tab A. Deception Event and Execution Schedule

Tab B. Feedback and Monitoring Procedures

Tab C. Task Organization

Figure D-4. Annotated Psychological Operations Appendix (continued)

Appendix 4 (Electronic Warfare) to Annex P (Information Operations) to OPORD No____

1. SITUATION

a. Enemy.

(1) Identify the vulnerabilities of enemy INFOSYS and EW systems.

(2) Identify the enemy capability to interfere with accomplishment of the EW mission.

b. Friendly.

(1) Identify friendly EW assets and resources that affect EW planning by subordinate commanders.

(2) Identify friendly foreign forces with which subordinate commanders may operate.

(3) Identify potential conflicts within the friendly electromagnetic spectrum, especially if conducting joint or multinational operations. Identify and deconflict methods and priority of spectrum distribution.

c. Attachments and Detachments.

(1) List the EW assets that are attached or detached.

(2) List the EW resources available from higher headquarters.

2. MISSION

State how EW will support IO objectives.

3. EXECUTION

a. Scheme of Support. State the EW tasks.

b. Tasks to subordinate units. Identify the EW tasks for each unit.

c. Coordinating Instructions.

(1) Identify EW instructions applicable to two or more units.

(2) Identify the requirements for the coordination of EW actions between units.

(3) Identify the emission control guidance.

4. SERVICE SUPPORT. Identify service support for EW operations.

5. COMMAND AND SIGNAL

a. Command.

b. Signal. Identify if any, the special or unusual EW-related communications requirements.

Figure D-5. Annotated Electronic Warfare Appendix

Appendix 5 (IO Execution Matrix) to annex P (Information Operations) to OPORD No_____

State the IO Objective in terms of the desired information operations effects.

Tasked Unit or System	IO Task	Time of TOT or Effect	Location	Remarks
• Unit • System • Delivery system • Weapon system	• List tasks by IO element	• Continuing • On order • NLT • Continuing • Per fire plan	• Unit location • Grid • Target	• EEFI • Deny • Influence Protect • Destroy

Special instructions.

Figure D-6. Annotated Information Operations Execution Matrix

Annex P (Information Operations) to XXI Corps OPORD 03-01

1. SITUATION

a. Enemy forces. See Appendix 1 (Initial IPB) to annex B (Intelligence).

b. Friendly forces.

(1) IO assets and resources needed.

(a) XXI Corps. E/151st Target Acquisition Det (Q37), A/322d MI Bn (ACE), C/305th MI Bn (UAV), 365 CA Bde, 408 CA Bn (-), 362d PSYOP Co.

(b) Theater. EC-130H, EC-130E, EA-6B, F-16CJ (HARM), AC-130 (Specter).

(2) Critical limitations are METT-TC dependent.

c. Civil considerations.

(1) San Anglos has a free press.

(2) Most San Anglos homes have radio.

(3) Most citizens have access to TV.

d. Attachments and detachments. 362d PSYOP Co, 449th CA Bn, 2 x CA tms from 408th CA Bn.

2. MISSION. IO supports XXI Corps operations by preventing preemption of the air assault, influencing the local population not to interfere in and around the objective areas, and shaping the information environment to support efforts to establish order and provide basic services.

Figure D-7. Example Information Operations Annex

3. EXECUTION

a. Scheme of Support.

(1) **IO Concept of Support**. IO supports XXI Corps operations by preventing preemption of the air assault and by minimizing civil interference in and around the objective areas through destroying, degrading, disrupting, and exploiting Rendovan C2 and fire support systems; deceiving Rendovan decisionmakers; destroying, degrading, disrupting, and deceiving Rendovan ISR systems; denying Rendovan decisionmakers information about XXI Corps intentions and capabilities; protecting friendly C2 and INFOSYS; countering Rendovan propaganda and deception operations. CMO emphasizes the Government of San Anglos stay-put policy. IO supports the JTF and XXI Corps deception plans. IO objectives, in priority, are—

(a) Prevent compromise of the operation.

(b) Protect XXI Corps C2.

(c) Disrupt 109th Division ADA, ISR, C2, and targeting systems during critical periods of the operation.

(d) Minimize civilian interference in the objective area.

(2) **OPSEC** (see appendix 1, OPSEC). Prior to H-hour, prevent Tiger Corps commander from determining the XXI Corps mission. After H-hour, prevent Tiger Corps commander from determining the objectives of the air assault and the avenues of approach. Throughout, OPSEC emphasizes protecting HVTs and EEFI. EEFI include movement or staging sites, unit assembly areas, counterbattery radar sites, ADA radar locations, FARPs, location or movement of communications nodes, and ammunition storage sites. All elements conduct counterreconnaissance to protect HVTs. Protect the daily agendas for the CG, ADC-M, ADC-S, and COS.

(3) **PSYOP** (see appendix 2, PSYOP). PSYOP promotes the Government of San Anglos stay-put policy through leaflet and loudspeaker operations. PSYOP products will disseminate themes and messages coordinated with HQ JTF that stress civilian noninterference (“stay-put”), exploit Rendovan military failures and casualties, counter Rendovan propaganda, and sustain civilian morale in occupied areas. Surrender appeals to Rendovans will be continuous and focused on JTF successes and Rendovan failures/losses. Additionally, surrender appeals will include offers of shelter and food. PSYOP will also support the corps MD operation.

(4) **Military Deception** (see appendix 3, MD). The JTF deception operation is attempting to convince Rendovan national decisionmakers that the US is using San Anglos as a staging area for an invasion of Rendova that will be spearheaded by the IV MEF, which is off shore in the Strait of Dawaro. It is supported by a national-level PSYOP campaign. The XXI Corps MD operation complements the JTF and national deception operations by portraying XXI Corps as preparing for an air and amphibious assault across the Strait of Dawaro.

Figure D-7. Example Information Operations Annex (continued)

(5) **Electronic Warfare** (see appendix 4, EW). Before H-hour, EW supports the corps MD operation. After H-hour, EW supports SEAD to disrupt the Tiger Corps ADA targeting and C2.

(6) **Computer Network Operations**. Not applicable.

(7) **Computer Network Attack**. XXI Corps will forward CNA requests to JTF 250. Results will be provided to the commander and G-7.

(8) **Computer Network Defense** (see annex H, C4OPS). System managers will stress all protection and defensive measures.

(9) **Computer Network Exploitation**. Not applicable.

(10) **Physical Destruction** (see annex D, Fire Support). Corps Artillery, and JTF fire support assets will support the air assault and MD operations. Critical C2 nodes will be destroyed at decisive points during the battle. Other INFOSYS and infrastructure that supports information transfer or that are useful to the enemy will be disrupted or degraded but will not be destroyed.

(11) **Information Assurance** (see annex H, C4OPS). Throughout the entire operation, the G-6 will monitor the TACWAN with an intrusion detection system for malicious codes, viruses and hacking activities. The G-6 will enforce XXI Corps INFOSYS security in accordance with the XXI Corps Security SOP. Computer users will receive periodic information systems security/OPSEC awareness reminders at the formal staff update, by email, and on the TACWAN web page.

(12) **Physical Security** (see annex K, Provost Marshal). Throughout the operation, elements in the JRA will conduct aggressive counterreconnaissance to search out and destroy all SPF and to protect critical C2 nodes and LOCs. MPs will integrate the stay-put policy and their counterincursion operations (combat patrols to find and destroy SPF) into the rear area force protection plan. MPs will establish a timely and recurring exchange of information collected on SPF HUMINT with HN police/security forces, counterintelligence, and the CMOC.

(13). **Counterintelligence** (see annex B, Intelligence). Counterintelligence assets will support force protection and identify SPF activities through obtaining information from civilians, liaison with San Anglos police forces and established source operations. CI/IPW will establish a timely recurring exchange of information collected on SPF with CA, MP, and XXI Corps main IO cell.

(14) **Counterdeception** (see annex B, Intelligence). Counterdeception activities will forewarn subordinate unites of Rendovan deception operations and exploit their deception.

(15) **Counterpropaganda** (see appendix 2, PSYOP). XXI Corps PSYOP units will broadcast messages countering Rendovan propaganda. Themes will emphasize the unity of San Anglos and how well ethnic Rendovans have fared under the current regime. Additionally, in accordance with JTF PAO, PA will present the international and US press with accurate information on JTF and ASA operations.

Figure D-7. Example Information Operations Annex (continued)

(16) **Civil-Military Operations** (see annex U, CMO). Support the stay-put policy throughout the operation. Coordinate with SJA for ROE/local restrictions. Priority is to establish links with Rendovan civil-military organizations. Coordinate with PSYOP, MP, CI, and IPW assets to provide composite teams at DC collection points and camps. Coordinate with PSYOP for DC control messages.

(17) **Public Affairs**. (See annex V, Public Affairs). PA will coordinate information about the stay-put policy with the San Anglos media. The internal [formerly command] information program will focus on such issues as force protection, protecting EEFI, and information on other command-emphasized issues. The internal information program will also provide facts on casualties and selected events on a timely basis to preempt propaganda, misinformation, and rumors. Embedded media support will include plans for operations in an NBC environment. Priorities are (1) emphasizing the lead role played by the ASA, (2) publicizing XXI Corps successes and enemy failures, and (3) conveying US resolve and overwhelming combat capability. PA will provide support and access to the national and international media as appropriate.

b. Tasks to subordinate units. See Appendix 5 (Execution Matrix).

c. IO Cell.

(1) The IO cell consists of representatives from all IO elements and coordinating staff sections.

(2) Facilitate integration and coordination of the stay-put policy for the purpose of locating/targeting SPF and providing support to OPSEC, MD operations, and force protection.

(3) Assist subordinates in planning/coordinating their IO missions.

(4) Analyze information reported through the stay-put policy, and other operational sensors. Ensure collated information is provided to the intelligence collection plan manager. Assist in verifying the accuracy of the identification/reports. Facilitate the timely dissemination of this information to the tactical operations watch officer.

(5) Meet per SOP.

d. Coordinating Instructions.

(1) XXI Corps will contact their San Anglos PA, CMO, PSYOP, CI/IPW, and MP counterparts to coordinate and synchronize efforts to identify and report suspected SPF locations and movements. IO will coordinate and synchronize EW, PSYOP, and physical destruction to disrupt or degrade Tiger Corps C2 nodes and other INFOSYS affecting the Rendovan decisionmaking process. During the air assault, IO will minimize DC interference, and support the XXI Corps MD plan. The XXI Corps IO cell will integrate the actions of PA, CMO, PSYOP, MP, NGOs, ISR, base security, force protection, and OPSEC into a single coordinated effort to support the Government of San Anglos stay-put policy. Efforts include—

Figure D-7. Example Information Operations Annex (continued)

(a) Integrate the XXI Corps “Neighborhood Partnership” program with existing San Anglos procedures used by citizens to report suspected enemy activity.

(b) Build cooperation and support for the stay-put policy among the local population, local media, humanitarian assistance groups, local law enforcement, and San Anglos governmental agencies.

(c) Establish and widely publicize central locations and telephone numbers throughout the XXI Corps AO for citizens and others to use to report information on suspected SPF activity.

(d) Provide centralized locations for displaced citizens to receive food and shelter from NGOs operating in XXI Corps AO.

(e) Build public support through open and responsive media relations, both in San Anglos and in the United States, for the XXI Corps participation in the conflict.

(2) XXI Corps IO Cell. G-7 will brief the effectiveness of the stay-put policy and other IO activities at the XXI Corps formal staff update briefing.

4. SERVICE SUPPORT. See annex I, Service Support.

5. COMMAND AND SIGNAL

a. Command.

(1) The G-7 reports IO significant activity to COS.

(2) XXI Corps will centrally coordinate assets to be used in an IO role.

(3) The XXI Corps IO cell is located in the main CP.

b. Signal. See annex H, C4OPS.

Appendix 1, OPSEC.

Appendix 2, PSYOP

Appendix 3, Military Deception

Appendix 4, Electronic Warfare

Appendix 5, IO Execution Matrix

ACKNOWLEDGE

Figure D-7. Example Information Operations Annex (continued)

Appendix 4 (IO Execution Matrix) to Annex P (Information Operations) to OPORD No_____				
Tasked Unit or System	**IO Task**	**Time of TOT or Effect**	**Location**	**Remarks**
XXI Corps Artillery	PD-01	H – 5	Known and templated Tiger Corps ISR systems	Use latest targeting data from Corps and 121st ID G-2
XXI Corps G-6; 121st ID G-6; all unit S-6s	CND-01	Start at H – 48 and continue	Throughout AO	
XXI Corps PAO	PA-01	Start at H – 48 and continue	Throughout AO	Lack of coverage may show PSYOP message is working
XXI Corps units	PS-01	Start at H – 48 and continue	Throughout AO	Provost marshal provides info to COS
XXI Corps units and 121 ID units.	IA-01	Start at H – 48 and continue	Throughout AO	
21st MI Bde	PSY-01	H – 24	AO Courtney	Successful if DCs stay off roads
21st MI Bde	MD-01	Start at H – 48 and continue	HQ Tiger Corps	
21st MI Bde	CI-01	Start at H – 48, one sortie every 10 hours	Throughout AO	
21st MI Bde/ 121st MI Bn	EW-01	H-hour	Tiger Corps communications interception and locating systems	Use latest targeting data from XXI Corps and 121st ID G-2
365th CA Bde	CMO-01	Start at H – 48 and continue	Throughout AO	
1st Bn, 19th PSYOP Grp	PSY-01	H – 24	AO Courtney	Successful if civilians stay off roads

Figure D-8. Example Information Operations Execution Matrix (extract)

Appendix E

Information Operations Targeting

This appendix discusses applying the targeting process to developing and engaging information-operations-related targets. It is organized around the four targeting functions: decide, detect, deliver, assess. It discusses the decide function in terms of military decisionmaking process tasks. This appendix supplements the tactics, techniques, and procedures that FM 6-20-10 establishes for the targeting process. Refer to FM 6-20-10 for targeting process details and examples of targeting products.

THE TARGETING PROCESS AND TARGETING TEAM

E-1. Targeting is a logical process that synchronizes lethal and nonlethal fires with the effects of other battlefield operating systems. It is an integral part of Army operations. Based on the commander's targeting guidance and targeting objectives, the targeting team determines what targets to attack and how, where, and when to attack them. It then assigns targets to systems best suited to achieve the desired effects. The chief of staff/executive officer leads the targeting team. Fire support, G-2, G-3, and Air Force representatives form its core. Other coordinating and special staffs participate, as their functional areas require. A G-7 representative attends all targeting team meetings, submits information-operations-related targets, and integrates information operations (IO) factors into the targeting process.

E-2. Targeting supports both offensive IO and defensive IO. Engaging IO-related targets contributes to achieving such offensive IO objectives as—

- Destroy, degrade, disrupt, deny, deceive, and exploit adversary command and control (C2) systems.
- Degrade or influence adversary morale and will to fight.
- Influence adversary decisionmakers.
- Influence the local population to support the command's mission.

Targeting for defensive IO supports protecting friendly units and decisionmakers; their decisionmaking processes, information, and information systems; and friendly/neutral populations.

CONTENTS

E-3. The Army targeting methodology is based on four functions: decide, detect, deliver, and assess (see figure E-1). The *decide* function occurs concurrently with planning. The *detect* function occurs during preparation and execution. The *deliver* function occurs primarily during execution, although some IO-related targets may be engaged while the command is preparing for the overall operation. The *assess* function occurs throughout the operations process but is most intense during execution.

	Operations Process Activity	Targeting Process Function	Targeting Task
ASSESSMENT	PLANNING	DECIDE	**Mission Analysis** • Develop IO-related HVTs • Provide IO input to targeting guidance and targeting objectives **COA Development** Designate potential IO-related HPTs Contribute to TVA Deconflict and coordinate potential HPTs **COA Analysis** Develop HPTL Establish TSS Develop AGM Determine criteria of success BDA requirements **Orders Production** Finalize HPTL Finalize TSS Finalize AGM Submit IO IRs/RFIs to G-2
	PREPARATION EXECUTION	DETECT	• Execute collection plan • Update PIRs/IO IRs as they are answered • Update HPTL and AGM
		DELIVER	• Execute attacks in accordance with the AGM
		ASSESS	• Evaluate effects of attacks • Monitor targets attacked with nonlethal IO

Figure E-1. Targeting Process Activities and Tasks

E-4. The targeting process is cyclical. The command's battle rhythm determines the frequency of targeting team meetings. The G-7 schedules internal targeting meetings so IO-related target nominations arrive within the command's target nomination windows. To conserve time, the G-7 may hold IO targeting meetings concurrently with IO cell meetings. Figure E-2 shows an example of an IO schedule that fits a command's battle rhythm.

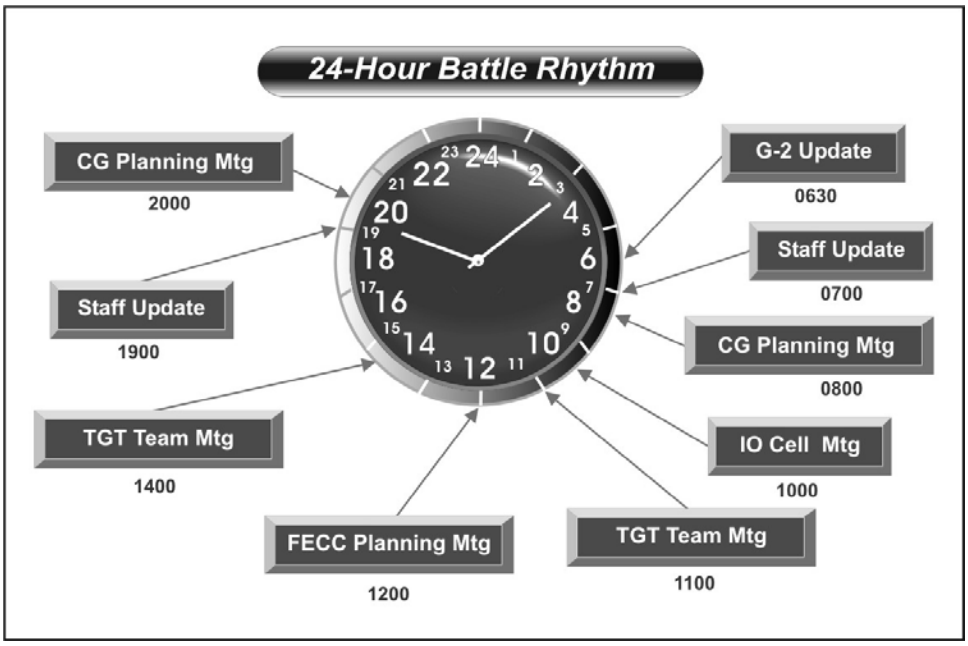


Figure E-2. Information Operations Targeting and Battle Rhythm

DECIDE

E-5. The decide function is part of the planning activity of the operations process. It occurs concurrently with the military decisionmaking process (MDMP). During the decide function, the targeting team focuses and sets priorities for intelligence collection and attack planning. Based on the commander's intent and concept of operations, the targeting team establishes targeting priorities for each phase or critical event of an operation. The following products reflect these priorities:

- **High-payoff target list**. The high-payoff target list (HPTL) is a prioritized list of high-payoff targets. A *high-payoff target* is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action (COA). High-payoff targets are those high-value targets (see definition at paragraph E-6), identified through wargaming, that must be acquired and successfully attacked for the success of the friendly commander's mission (JP 1-02). IO-related high-payoff targets (HPTs) are C2 nodes and intelligence collection apparatuses.
- **Intelligence collection plan**. The intelligence collection plan, prepared by the G-2 and coordinated with the G-3, integrates intelligence, surveillance, and reconnaissance (ISR) to answer the priority intelligence requirements (PIRs) (see FM 34-2). It is a major contributor to the detect and assess functions.
- **Target selection standards**. Target selection standards (TSS) establish criteria for deciding when targets are located accurately enough to attack. (See FM 6-20-10).

- **Attack guidance matrix**. The attack guidance matrix (AGM) lists targets or target categories, specific HPTs, when targets should be attacked, how they should be attacked, and any restrictions (see FM 6-20-10).
- **Target synchronization matrix**. The target synchronization matrix (TSM) is a list of HPTs by category and the agencies responsible for detecting them, attacking them, and assessing the effects of the attacks. It combines data from the high-payoff target list, intelligence collection plan and attack guidance matrix.

The targeting team develops or contributes to these products throughout the MDMP. The commander approves them during COA approval. The G-7 ensures they include information necessary to engage IO-related targets. IO-related vulnerability analyses done by the G-2 and the G-7 provides a basis for deciding which IO-related targets to attack. (See chapters 1 and 5 for the desired effects for offensive and defensive IO.)

E-6. A *high-value target* is a target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. (JP 1-02). During mission analysis and COA development, the G-7 develops IO-related high value targets (HVTs) concurrently with IO objectives and IO tasks. Not all IO tasks are candidates for the targeting process. During COA analysis the G-7 determines which IO-related HVTs should be HPTs and refines IO input to the AGM and TSS. The G-7 integrates IO objectives, IO tasks, and IO-related targets to ensure successful accomplishment of the IO mission.

MISSION ANALYSIS

E-7. The two targeting-related G-7 products of mission analysis are a list of IO-related HVTs and recommendations for the commander's IO targeting guidance. The G-7 works with the G-2 during intelligence preparation of the battlefield (IPB) to develop IO-related HVTs. The G-7 works with the targeting team to develop IO targeting guidance recommendations.

Intelligence Preparation of the Battlefield

E-8. IPB includes preparing doctrinal templates that portray adversary forces and assets unconstrained by the environment. The G-2 adjusts doctrinal templates based on terrain and weather to create situational templates that portray possible adversary COAs. These situational templates allow the G-2 to identify HVTs. The G-7 works with the G-2 throughout IPB to identify IO capabilities and vulnerabilities of adversaries and other key groups in the AO. These capabilities and vulnerabilities become IO-related HVTs.

Targeting Guidance

E-9. The commander's guidance, issued at the end of mission analysis, includes targeting guidance. Targeting guidance describes the desired effects of lethal and nonlethal fires. It is expressed in terms of targeting objectives (limit, disrupt, delay, divert, or destroy) or IO effects (destroy, degrade, disrupt, deny, deceive, exploit, or influence). Targeting focuses on essential adversary capabilities and functions, such as, the ability to form a hostile

crowd, mobilize, exercise C2 of forward units, or mass artillery fires. IO targeting focuses on HVTs the adversary needs to keep friendly forces from achieving their IO objectives.

E-10. The G-7 develops IO input to targeting guidance based on the initial IO mission and IO-related tasks. It identifies the function, capability, or units to be attacked; the IO effects desired; and the purpose for the attack. The G-7 uses the IO targeting guidance to select IO-related HPTs from the high-value target list. These HPTs are confirmed during COA analysis.

E-11. Targeting guidance is developed separately from IO objectives. IO objectives are generally broad in scope. They encompass both offensive and defensive IO, and often require both lethal and nonlethal means to accomplish. The G-7 develops recommendations for IO targeting guidance that support achieving IO objectives.

E-12. When developing IO input to the targeting guidance, the G-7 considers the potentially long lead time required to achieve effects from offensive IO and the possible lag time in determining results. Some IO elements may require targeting guidance that allows for the acquisition, engagement, and assessment of targets while the unit is preparing for the overall operation. For example, the commander may want to psychologically and electronically isolate an adversary reserve before engaging it with lethal fires. Doing this could require electronic attack (EA) of adversary C2 systems and psychological operations (PSYOP) directed at adversary soldiers 24 to 48 hours before the strikes. Successfully achieving the IO objectives for that phase of the operation requires targeting guidance that gives IO-related targets the appropriate priority.

COURSE OF ACTION DEVELOPMENT

E-13. During COA development, the staff prepares feasible COAs that integrate the effects of all elements of combat power to accomplish the mission. The G-7 prepares an IO concept of support that identifies IO objectives, and IO tasks required to achieve them, for each COA. IO-related targets are developed and coordinated as IO tasks (see figure E-3, page E-6).

E-14. When achieving an IO objective requires engaging an HVT, the G-7 designates that HVT as a potential IO-related target. The G-7 treats IO-related targets as IO tasks when preparing IO input worksheets. IO-related targets that are approved for engagement become HPTs. This determination is made during COA analysis.

E-15. During COA development, the targeting team performs target value analysis (TVA), coordinates and deconflicts targets, and establishes assessment criteria. The G-7 participates in each of these tasks.

Target Value Analysis

E-16. The targeting team performs TVA for each COA the staff develops. The initial TVA sources are target spread sheets and target sheets.

E-17. *Target spreadsheets* identify target sets associated with adversary functions that could interfere with each friendly COA or that are key to adversary success. The fire support element (FSE) usually prepares them. IO-related

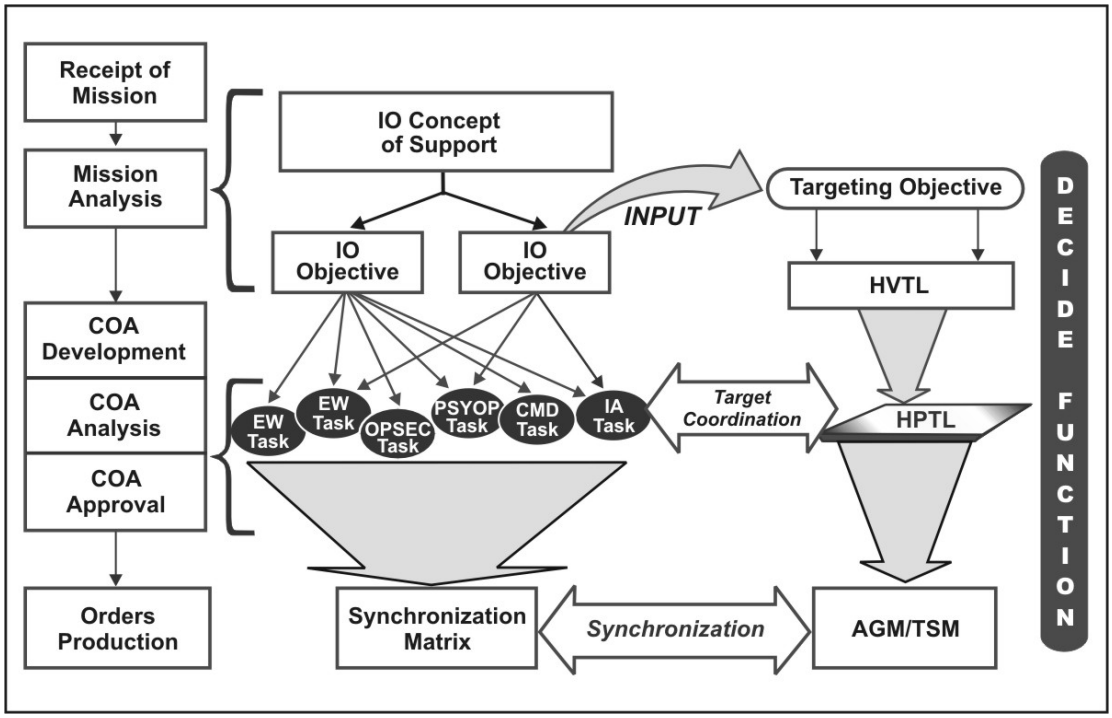


Figure E-3. Planning Information-Operations-Related Targets

targets can be analyzed as a separate target set or can be incorporated into other target sets. The G-7 and fire support coordinator (FSCOORD) determine which technique fits the situation. The G-7 establishes any IO-specific target sets. Each target set—including the IO target set, if designated—is assigned a priority (also called relative worth or relative value), based on how it contributes to the adversary COA being considered. The targeting team uses target spreadsheets during the war game to determine which HVTs to attack. The G-7—

- Ensures that target spreadsheets include information on adversary IO assets and IO-related HVTs.
- Ensures the IO target set, if designated, is assigned a value appropriate to IO's relative importance to each friendly COA. If an IO target set is not designated, the G-7 ensures that IO-related targets are assigned an appropriate priority within the target sets used.

E-18. A *target sheet* contains the information required to engage a target. It is a locally produced product. Target sheets state how attacking the target would affect the adversary operation. The G-7 prepares target sheets for IO-related HVTs to analyze them from an IO perspective. These HVTs are expressed as target subsets, such as decisionmakers. Information requirements (IRs) concerning them include—

- Influences on them.
- How they communicate.
- With whom they communicate.
- Weakness, susceptibility, accessibility, feasibility, and pressure points.

Deconflicting and Coordinating Targets

E-19. Members of the IO cell nominate IO-related targets and advise the G-7 on possible consequences of attacking them. Deconflicting the effects of attacking some IO-related targets is more complex than deconflicting the effects of lethal fires. IO often seeks to influence civilian audiences. Sometimes the act of engaging a target may have as great an effect as actually destroying it. Civil-military operations (CMO), public affairs (PA), and PSYOP personnel evaluate the advantages gained from engaging IO-related targets in those terms. Attacking some targets may have legal consequences; the staff judge advocate representative evaluates IO-related targets from that perspective. If engaging an IO-related target might result in effects outside the AO, the G-7 clears that target with higher headquarters.

E-20. IO cell members consider all targets from their IO element's perspective. Deconfliction in this context means making sure that engaging a target does not produce effects that interfere with the effects of other IO tasks or IO-related targets, or otherwise inhibit mission accomplishment. Coordination means making sure that the effects of engaging different targets complement each other and further the commander's intent. G-7s at different echelons may engage the same targets or may desire different effects. Therefore, IO targeting includes coordinating and deconflicting targets with higher and subordinate G-7s before the targeting team meets. Some IO-related targets may also be nominated by other staff elements. The G-7 presents the effects required to accomplish the IO objective associated with those targets when the targeting team determines how to engage them.

E-21. One way to achieve this coordination and deconfliction is by beginning parallel planning as early as possible in the MDMP. The G-7 and the targeting team share all pertinent information with subordinate units and adjacent and higher headquarters.

Assessment Criteria

E-22. Generally, the effects of lethal attacks can be evaluated using objective, quantifiable criteria, such as the percentage of the target that is destroyed. The G-7 requests battle damage assessment (BDA) of these targets. However, evaluating nonlethal attacks may require subjective criteria and monitoring the target over time. Establishing meaningful criteria of success requires understanding the desired end state. Evaluating effects in terms of subjective criteria requires interpreting information that portrays qualitative effects and determining how these effects change over time.

E-23. IO-related targets attacked by nonlethal fires, such as jamming or PSYOP broadcasts, may require assessment by means other than those normally used in BDA. The G-7 develops criteria of success for these targets and determines the information needed to determine how well they have been met. The G-7 prepares IO IRs or requests for information (RFIs) for this information. If these targets are approved, the IO IRs and RFIs needed to assess the effects on them become PIRs that the G-2 adds to the collection plan. If the command does not have the assets to answer these IO IRs, the target is not engaged unless the attack guidance specifies otherwise or the commander so directs. BDA can be obtained from various sources:

- G-2 provides feedback on the effects electronic warfare.
- G-3 provides feedback on the effects of disrupting C2 by reconnaissance units.
- G-5 provides feedback on the effectiveness of CMO.
- Public affairs officer provides feedback on how the operation is being reported in the international media.

COURSE OF ACTION ANALYSIS

E-24. COA analysis (war-gaming) is a disciplined process that staffs use to visualize the flow of a battle. During the war game, the staff decides or determines—

- Which HVTs are HPTs.
- When to engage each HPT.
- Which system to use against each HPT.
- The desired effects of each attack, expressed in terms of the targeting objectives or IO effects.
- Which HPTs require BDA. The G-7 submits BDA requirements for IO-related targets to the G-2 for inclusion in the collection plan.
- Which HPTs require special instructions or require coordination.

E-25. Based on the war game, the targeting team produces the following draft targeting products for each COA:

- High-payoff target list.
- Target selection standards.
- Attack guidance matrix.
- Target synchronization matrix.

High-Payoff Target List

E-26. During the war game, the staff determines which HVTs are HPTs for each COA. HPTs are critical to both the adversary's needs and the friendly concept of operations. They support achieving the commander's intent and executing the concept of operations. They are determined based on the commander's targeting guidance. The HPTL is a prioritized list of HPTs.

E-27. One way to organize the HPTL is to group all HPTs into target sets that reflect the capabilities and functions described in the targeting objectives. Thus, if the commander's targeting guidance is to "Delay the adversary force's ability to move mechanized forces across river Y to allow their destruction by air and artillery fires," then two target sets could be the following: "the ability to conduct a river crossing" and "C2 of mechanized forces listing specific nodes or pieces of equipment to cause a specific effect at a specific time and place." Target sets are identified and prioritized for each phase of the operation. Within the sets, individual targets are rank-ordered by target value, sequence of appearance, importance, or other criteria that satisfy the targeting objectives. In this way, the targeting team reduces, modifies, and reprioritizes HVTs while ensuring that HPTs support the concept of operations.

Target Selection Standards

E-28. TSS are criteria applied to adversary activities (acquisitions or combat information) to decide whether the activity can be engaged as a target. TSS are usually disseminated as a matrix. Military intelligence analysts use TSS to determine targets from combat information and pass them to FSEs for attack. Attack systems managers, such as fire control elements and fire direction centers, use TSS to determine whether to attack a potential target. The G-2 and FSCOORD determine TSS. The G-7 ensures that they consider IO-related targets and establish appropriate standards for engaging them.

E-29. For nonlethal attacks, the G-7 may have to develop descriptive criteria to supplement or replace criteria developed by the FSE. For example, nonlethal TSS during a peace operation may describe what constitutes a hostile crowd (such as, a group larger than 25 people, armed with sticks or other weapons, and with leaders using radios or cellular telephones to direct it). To do this, the G-7 identifies specific pressure points, such as one's credibility. The G-7 then attacks these pressure points with specific means/products, delivered to a specific communications node or system, to cause a specific effect.

Attack Guidance Matrix

E-30. The targeting team recommends attack guidance based on the results of the war game. Attack guidance is normally disseminated as a matrix (the AGM). An AGM includes the following information, listed by target set or HPT:

- Timing of attacks (expressed as immediate, planned, or as acquired).
- Attack system assigned.
- Attack criteria (expressed as neutralize, suppress, harass, or destroy).
- Restrictions or special instructions.

E-31. Only one AGM is produced for execution at any point in the operation; however, each phase of the operation may have its own matrix. To synchronize lethal and nonlethal fires, all lethal and nonlethal attack systems, including PSYOP and EA, are placed on the AGM. The AGM is a synchronization and integration tool. It is normally included as part of the fire support annex. However, it is not a tasking document. Attack tasks for unit assets, including IO elements, are identified as taskings to subordinate units and agencies in the body or appropriate annexes or appendixes of the operation plan (OPLAN)/operation order (OPORD).

Target Synchronization Matrix

E-32. The TSM lists HPTs by category and the agencies responsible for detecting them, attacking them, and assessing the effects of the attacks. It combines data from the HPTL, intelligence collection plan, and AGM. A completed TSM allows the targeting team to verify that assets have been assigned to each targeting process task for each target. The targeting team may prepare a TSM for each COA, or may use the HPTL, TSS, and AGM for the war game and prepare a TSM for only the approved COA.

COA COMPARISON, COA APPROVAL, AND ORDERS PRODUCTION

E-33. After war-gaming all the COAs, the staff compares them and recommends one to the commander for approval. When the commander approves a COA, the targeting products for that COA become the basis for targeting for the operation. The targeting team meets to finalize the HPTL, TSS, AGM, and input to the collection plan. The team also performs any additional coordination required. After accomplishing these tasks, targeting team members ensure that targeting factors that fall within their functional areas are placed in the appropriate part of the OPLAN/OPORD.

DETECT

E-34. The *detect* function involves locating HPTs accurately enough to engage them. It primarily entails execution of the intelligence collection plan. Although the G-2 oversees the execution of intelligence collection plan, the collection assets themselves do not all belong to the G-2. All staff agencies, including the G-7, are responsible for passing to the G-2 information collected by their assets that answer IRs. Conversely, the G-2 is responsible for passing combat information and intelligence to the agencies that identified the IRs. Sharing information allow timely evaluation of attacks, assessment of IO, and development of new targets. Effective information management is essential.

E-35. The intelligence collection plan focuses on identifying HPTs and answering PIRs. These are prioritized based on the importance of the target or information to the commander's concept of operation and intent. PIRs can include IO IRs, as designated by the commander; these priority intelligence collection requirements will assist the G-7 in assessing IO. Thus, there is some overlap between detect and assess functions. Detecting targets for nonlethal attacks may require ISR support from higher headquarters. The targeting team adjusts the HPTL and AGM to meet changes as the situation develops. The G-7 submits new IO IRs/RFIs as needed.

DELIVER

E-36. The *deliver* function involves engaging targets located within the TSS according to the guidance in the AGM. HPT that are located within the TSS are tracked and engaged at the time designated in the OPORD/AGM. Other collection assets look at HPTs that are not located accurately enough or for targets within priority target sets. When one of these is located within the TSS, its location is sent to the system that the AGM assigns to attack it. All HPTs will not be identified accurately enough to be attacked before execution. Some target sets may not have very many targets identified. Collection assets and the intelligence system develop information that locates or describes potential targets accurately enough to engage them. The HPTL sets the priority in which they accomplish this task.

ASSESS

E-37. Assessment occurs throughout the operations process. The effects of lethal attacks on IO-related targets are assessed the same way as other fire

support or EA targets. Targets are reattacked until the effects outlined in the AGM are achieved or until the target is no longer within the TSS (see FM 6-20-10).

E-38. The effects of nonlethal attacks on IO-related targets require continuous assessment. The G-7 is responsible for this assessment and monitors reporting based on IO IRs and RFIs submitted during planning (the decide function). IO elements/related activities with close contact with the civilian populace—such as counterintelligence, PA, and CMO—can collect information about the effects of nonlethal IO by such IO elements as PSYOP and counterpropaganda. The G-7 uses the criteria of success established during COA analysis to evaluate IO effectiveness and monitors targets as required to maintain a continuous assessment. Based on this assessment, the G-7 decides whether to continue to engage the target, break off the attack, or engage the target with another IO element. This decision is based on the extent to which continuing to engage the target will further accomplishing the IO objectives it supports and the extent to which accomplishing the IO objectives will contribute to accomplishing the mission.

E-39. The large amount of information generated during operations means target attack effects may be difficult to capture. The G-2, G-3, and G-7 work closely to develop meaningful, timely BDA of IO-related targets. The G-7 establishes mechanisms and procedures with other staff elements, particularly the G-2, that allow exploitation of real-time data to support timely assessment of IO targeting. In a digitized division, this may include using the Maneuver Control System–Light (MCS-light). (See figure B-26, pages B-39–B-42, for an example of an IO assessment matrix).

SUMMARY

E-40. The G-7 develops IO-related targets that support achieving IO objectives. Throughout the MDMP, the G-7 integrates IO planning with the targeting process. During preparation and execution, the G-7 monitors BDA and other reports to evaluate the effectiveness of IO against IO-related targets and to assess the overall effects of IO.

Appendix F

Staff Responsibilities and Supporting Capabilities

Appendix F lists information-operations-related responsibilities of staff sections at Army service component command, corps, division, and brigade levels. It also describes the capabilities of, and support available from, selected Army commands. Figure 1-2, page 1-15, shows the relationship between the IO elements/related activities, the types of operations, and unit responsibilities.

CORPS AND DIVISION INFORMATION OPERATIONS RESPONSIBILITIES

F-1. Corps and divisions have organic G-7 sections. G-7 sections—supervised by the assistant chief of staff (ACOS) G-7—plan, assess, and oversee preparation and execution of information operations (IO). The ACOS G-7 exercises coordinating staff responsibility over the following special staff officers: electronic warfare officer (EWO), military deception officer (MDO), operations security (OPSEC) officer, and psychological operations (PSYOP) officer. They have the following responsibilities.

ASSISTANT CHIEF OF STAFF, G-7 (INFORMATION OPERATIONS)

F-2. The G-7 is the coordinating staff officer for all IO matters, including current operations, plans, and IO-related targeting. He is a functional area 30 officer. A G-7 is authorized at Army service component commands (ASCCs), corps, and divisions. Selected Army National Guard and active component brigades are authorized an S-7.

CONTENTS

Current Operations

F-3. FM 6-0 establishes the following general G-7 (S-7) responsibilities related to current operations:

- Ensure IO supports achieving information superiority.
- Synchronize and coordinate offensive and defensive IO with the overall operation.
- Assess the effects of offensive and defensive IO throughout the operations process; recommend IO adjustments as required.
- Coordinate and synchronize tactical IO with theater-strategic- and operational-level IO.
- Coordinate IO elements and related activities for the chief of staff (COS) or executive officer (XO).
- Integrate intelligence from the G-2 (S-2) into IO.
- Coordinate the attachment of the 1st Information Operations Command (Land) (1st IOC [L]) field support teams and other specialized IO teams.
- Monitor execution by IO elements to ensure delivery of massed information effects when needed.

F-4. The following responsibilities clarify the G-7 (S-7) general current operations responsibilities established in FM 6-0:

- Request, through the G-3, IO resources from higher headquarters.
- Integrate IO into all current operations.
- Synchronize measures to protect friendly information and other IO capabilities from attack. The G-6, in coordination with the G-7, is responsible for information assurance (IA) management, computer network defense (CND) functions, and ensuring IA activities support IO objectives established in the IO annex. The G-7 supports IA by ensuring external vulnerability analyses are performed.
- Synchronize the capabilities of the IO elements.
- Coordinate with the ASCC and joint task force (JTF) staffs on IO matters (corps G-7).
- Coordinate with the corps G-7 and subordinate brigade headquarters on all IO matters (division G-7).
- Coordinate links to access/exchange information from military and nonmilitary sources.
- Prepare for or arrange augmentation to meet special needs and shortfalls of headquarters designated as ARFOR headquarters.
- Monitor the out-of -theater information environment.
- Monitor and recommend adjustment of collection of IO information requirements (IRs).
- Coordinate with G-2 to answer IO IRs.
- Maintain liaison with supporting military, governmental, and nongovernmental organizations to obtain IO IR answers not normally available at the tactical level.
- Act as a witting participant in military deception (MD) operations.
- Determine IO assets available from the higher headquarters.

Plans

F-5. FM 6-0 establishes the following general G-7 (S-7) responsibilities related to plans:

- Exercise staff coordination over the conduct of the overall IO effort.
- Coordinate preparation of the IO portions of plans and orders.
- Produce other IO products.
- Recommend priorities to accomplish IO tasks identified during planning.
- Leverage the capabilities of higher-echelon IO agencies and units providing connectivity with national- and theater-level IO agencies.

F-6. The following responsibilities clarify the G-7 (S-7) general planning responsibilities established in FM 6-0:

- Coordinate IO plans with higher and lower headquarters.
- Assess the effects of offensive and defensive IO throughout the operations process, modifying IO plans as required.
- Recommend appropriate IO IRs as commander's critical information requirements (CCIR).
- Act as a witting participant in MD operations.
- Develop IO objectives and tasks.
- Establish priorities for IO objective and tasks.
- Synchronize, coordinate, and deconflict planning for IO tasks.
- Produce other IO products for the commander and staff.
- Develop IO input to intelligence preparation of the battlefield (IPB).
- Integrate intelligence, surveillance, and reconnaissance (ISR) capabilities from the G-3 and G-2 into IO planning.
- Provide IO input to the G-3 plans cell with assistance of IO element subject matter experts.
- Develop IO plans within the commander's intent to support the concept of operations and achieve desired end state.
- Submit IO IRs that require intelligence-reach support to the G-2.

Targeting

F-7. FM 6-0 establishes the following general G-7 (S-7) responsibilities related to targeting:

- Participate in targeting meetings.
- Recommend IO effects to influence adversary perceptions, decisions, and actions.

F-8. The following responsibilities clarify the G-7 (S-7) general targeting responsibilities established in FM 6-0:

- Develop IO-related targets.
- Coordinate the nomination of IO-related targets with the G-2 analysis and control element (ACE).
- Provide input to IPB.
- Act as a witting participant in MD operations.
- Provide IO input into the targeting process.

- Provide IO input to target lists, estimates, and assessments.
- Receive input from out-of-theater and national information sources.
- Assist in deconflicting targets scheduled for electronic attack (EA) and ISR collection.
- Nominate IO targets for lethal and nonlethal attack.

Staff Planning and Supervision

F-9. The G-7 (S-7) has the following staff planning and supervision responsibilities:

- Establish and supervise IO cell.
- Coordinate IO with other agencies (such as, the US Information Agency, US Agency for International Development, and US ambassador).

ELECTRONIC WARFARE OFFICER

F-10. The EWO is normally a military intelligence officer who performs electronic warfare (EW) duties. An EWO is authorized at corps and divisions. EWO responsibilities established in FM 6-0 include—

- Coordinate with the G-7 to integrate EW into IO.
- Coordinate, prepare, and maintain the EW target list, EA taskings, EA requests, and the EW portion of the sensor/attack matrix.
- Coordinate with the G-6 to deconflict EW targets with frequencies and the joint restricted frequency list.
- Coordinate with the fire support coordinator (FSCOORD) and G-2 (ACE) to identify opportunities for conducting effective EA.
- Participate in targeting meetings.
- Analyze adversary EW activities (with the G-2).
- Assess adversary vulnerabilities, friendly capabilities, and friendly missions in EW terms.
- Develop a prioritized adversary C2 target list based on high-value targets (HVTs) and high-payoff targets (HPTs) (with the FSCOORD).
- Develop the EA mission tasking based on the command and control (C2) target list, and issue the EA target list.
- Coordinate the EA target list with organic military intelligence units and with adjacent and higher commands, including joint and multinational commands when appropriate.
- Coordinate with the higher headquarters EWO to deconflict IO on the communications spectrum.
- Help the G-6 determine electronic protection (EP) requirements.
- Prepare EW estimates and the EW appendix to the IO annex.
- Forward and coordinate electronic warfare support (ES) targets with the G-2. The G-2 collection manager integrates ES targets into the collection plan and the intelligence synchronization plan.
- Brief adversary and friendly EW vulnerabilities for each course of action (COA).

F-11. The following responsibilities clarify the G-7 (S-7) general EWO responsibilities established in FM 6-0:

- Recommend where EW should be considered during IO planning.

- Deconflict targets with the joint restricted frequency list.
- Provide a representative to the IO cell.
- Forward and coordinate ES targets with the G-2. The G-2 integrates ES targets into the collection plan and the intelligence synchronization plan.

MILITARY DECEPTION OFFICER

F-12. The MDO is a functional area 30 officer responsible for coordinating MD assets and operations. FM 6-0 establishes the following general MDO responsibilities:

- Exercise staff supervision over MD activities.
- Provide expertise in MD operations.
- Manage information required for conducting MD operations.
- Determine requirements or opportunities for MD operations (with the G-2).
- Recommend to the G-7 the deception target, deception objective, and deception story.
- Write the MD appendix to the IO annex.
- Coordinate operations security (OPSEC) measures to shield the MD plan with the OPSEC officer.
- Coordinate with the higher headquarters MDO and G-7, the engineer coordinator (ENCOORD), and the chemical officer (CHEMO).
- Distribute the MD plan on a need-to-know basis.
- Integrate MD assets.
- Assess execution of MD operations.

F-13. The following responsibilities clarify the general MDO responsibilities established in FM 6-0:

- Ensure all MD operations support the commander's intent.
- Monitor witting and unwitting participants involved in MD operations.
- Recommend who should participate in the deception working group (DWG).
- Provide a representative to the IO cell.
- Coordinate with the G-7 to ensure synergism of MD.
- Ensure other IO tasks do not conflict with MD operations and vice versa.
- Collect and process information on how potential deception targets exercise command and control.

OPERATIONS SECURITY OFFICER

F-14. The OPSEC officer helps the G-7 (S-7) perform OPSEC functions. Commanders at all echelons, battalion through corps, are authorized or appoint an OPSEC officer. Divisions and above are authorized a functional area 30 OPSEC officer. FM 6-0 establishes the following general OPSEC officer responsibilities:

- Conduct OPSEC assessments to analyze the command's OPSEC posture.

- Coordinate with higher headquarters for OPSEC activities support.
- Determine essential elements of friendly information (EEFI) and OPSEC vulnerabilities and recommend EEFI to the commander.
- Recommend OPSEC measures, based on weighing the risks to the mission against the cost of protection.
- Publish the OPSEC appendix to the IO annex.
- Coordinate with other members of the IO cell to ensure OPSEC coverage and dissemination of OPSEC measures.
- Submit taskings for OPSEC tasks to subordinate units through the G-7 to the G-3.
- Determine the effect of compromises of critical friendly information systems (INFOSYS), functions, and data.
- Coordinate with the 1st IOC (L) for IO vulnerability assessments and red-teaming.
- Evaluate effectiveness of force-protection measures (with the G-7, ENCOORD, and the CHEMO).
- Report incidents through channels to regional computer emergency response team and Army Computer Emergency Response Team (ACERT).

F-15. The following responsibilities clarify the general OPSEC officer responsibilities established in FM 6-0:

- Request support for IO vulnerability assessments, and red-teaming through the G-7 to the G-3.
- Request ACERT, and regional computer emergency response team (RCERT) support through the G-7 to the G-6.
- Coordinate with the G-2 to determine collection capabilities of adversaries.
- Provide a representative to the IO cell.

PSYCHOLOGICAL OPERATIONS OFFICER

F-16. The PSYOP officer is functional area 39 officer responsible for coordinating PSYOP operations. A PSYOP officer is authorized at corps and divisions. If no PSYOP officer is assigned, the commander of an attached PSYOP support element may assume the PSYOP officer's responsibilities. FM 6-0 establishes the following general PSYOP officer responsibilities:

- Coordinate with the G-7 to ensure synchronization of PSYOP.
- Synchronize command PSYOP with higher headquarters PSYOP.
- Write the PSYOP appendix to the IO annex.
- Perform staff planning and coordination of PSYOP activities.
- Conduct PSYOP to support the overall operation.
- Allocate organic and supporting resources to support PSYOP efforts.
- Prioritize the efforts of attached PSYOP forces.
- Evaluate enemy PSYOP efforts and the effectiveness of friendly PSYOP on target groups (with the G-2 and G-5).
- Coordinate possible PSYOP effects with the G-5.
- Coordinate support of dislocated civilian operations with the G-5.

- Coordinate audience pretesting and posttesting of propaganda and counterpropaganda products.
- Assess PSYOP effectiveness.
- Provide a representative to IO cell meetings.
- Assess the psychological impact of military operations on the enemy and the civilian populace.
- Counter enemy propaganda and misinformation.
- Coordinate with the public affairs officer (PAO) and G-5 to ensure disseminated messages are consistent.

F-17. The following responsibilities clarify the general PSYOP officer responsibilities established in FM 6-0:

- Provide PSYOP expertise.
- Coordinate with the G-2 to determine the following:
  - Shared ideologies among potential adversaries.
  - Funding of adversary activities.
  - Order of battle of potential adversaries.

OTHER STAFF OFFICER INFORMATION OPERATIONS RESPONSIBILITIES

F-18. In addition to the staff responsibilities listed in FM 6-0, the following staff officers have IO-related responsibilities.

Chief of Staff

F-19. The COS (the XO at brigades and battalions) is the commander's principal assistant for directing, coordinating, supervising, and training the staff, except in areas the commander reserves. IO-related responsibilities of the COS (XO) are—

- Ensure information superiority is accomplished at times and places the commander designates.
- Ensure that the information element of combat power is integrated into operations as stated in the commander's intent and concept of operations. At corps, divisions, and selected brigades, the G-7 (S-7) and other coordinating staff officers assist the COS (XO) with IO responsibilities.
- Ensure IO is executed along with information management (IM) and ISR to accomplish information superiority.
- Chair targeting meetings.
- Act as a witting participant in MD operations.

Assistant Chief of Staff, G-1/AG (Personnel)

F-20. The ACOS G-1/AG is the principal staff officer for personnel functions. IO-related responsibilities of the G-1 are—

- Coordinate with the ACOS G-7 on IO matters.
- Provide a representative to the IO cell.
- Conduct personnel support of IO.
- Provide IO instructions in the personnel appendix of the service support annex.
- Perform personnel manning functions prescribed in FM 12-6.

- Review IO mission and METT-TC considerations from personnel support perspective.
- Advise the MDO on availability of personnel resources required for the MD operation.
- Act as either a witting or unwitting participant in MD operations.

Assistant Chief of Staff, G-2 (Intelligence)

F-21. The ACOS G-2 is the principal staff officer for all matters concerning military intelligence, counterintelligence, security operations, and military intelligence training. The G-2 produces the intelligence used by the G-7 and his special staff officers. IO-related responsibilities of the G-2 are—

- Coordinate with the ACOS G-7 on IO matters.
- Participate in IO cell meetings.
- Provide IO instructions in intelligence annex.
- Provide information on adversary C2 systems for vulnerability assessments.
- Contribute to EA detection by providing warning and assessment of potential adversary activities, and by cueing collection to specific activity indicators.
- Include IO RFI from the G-7 in intelligence reach.
- Answer IO IRs.
- Coordinate with counterintelligence; law enforcement; and INFOSYS developers, providers, administrators, and users to ensure timely sharing of relevant information (RI).
- Prepare a vulnerability assessment of adversary C2 systems. Include—
  - Political, economic, social, and cultural influences.
  - Targets and methods for offensive operations.
  - Adversary (or potential adversary) decisionmaking processes.
  - Biographical backgrounds of key adversary leaders, decisionmakers, and communicators, and their advisors. Include motivating factors and leadership styles.
  - IPB of adversary C2 systems and INFOSYS.
  - A comprehensive comparison of adversary offensive IO capabilities against friendly IO vulnerabilities.
- Collect data to establish an EW database and C2 target list.
- Provide intelligence support to MD operations; specifically—
  - Determine adversary INFOSYS through which information reaches the deception target.
  - Help the G-6 plan use of friendly INFOSYS as deception means.
  - Establish counterintelligence measures to protect the MD operation from detection.
- Support computer network attack (CNA) requests with assessments.

Assistant Chief of Staff, G-3 (Operations)

F-22. The ACOS G-3 is the principal staff officer for all matters concerning training, operations and plans, and force development modernization. The G-3

synchronizes tactical operations and has staff responsibility for orders preparation. IO-related responsibilities of the G-3 are—

- Tasks units and assets to accomplish information superiority.
- Provide plans and current operations briefings to IO cell meetings.
- Request IO resources from higher headquarters upon recommendation from G-7. After allocations are made, pass coordination responsibility to the G-7.
- Integrate ISR into operations being supported by the G-2 (with the COS).
- Integrate space support, IO (with the G-7), and fire support into all operations.

The ACOS G-3 exercises coordinating staff responsibility over the following special staff officers with IO-related responsibilities.

F-23. **Chemical Officer.** The CHEMO has staff responsibility for nuclear, biological, and chemical (NBC) defense; smoke operations; and the use of chemical assets. IO-related responsibilities are—

- Coordinate with the PSYOP officer and G-7 when adversaries have the capability to use weapons of mass destruction.
- Provide a representative to the IO cell.
- Provides IO instructions in the chemical annex.
- Include IO aspects in the NBC defense and obscurant employment appendixes to orders and plans.

F-24. **Space Operations Officer.** The space operations officer provides space-related tactical support and coordinates space-based capabilities available to the command. IO-related responsibilities are—

- Coordinate with the Army space support team to provide space-based products to support IO requirements.
- Provide a representative to the IO cell.
- Include IO requirements in the space operations appendix to the operations annex.
- Coordinate IO requirements with higher headquarters for US Army Space Command and US Strategic Command support.
- Coordinate with the IO targeting officer to include adversary space-system elements in the targeting process.
- Support OPSEC and MD efforts by maintaining the adversary space order of battle, to include monitoring orbital paths and satellite coverage areas.
- Monitor space architecture (the hardware, systems and feedback mechanisms) availability in the areas of communications; position/navigation; space-based surveillance/warning; and weather, terrain, and environmental monitoring (WTEM).
- Conduct operational planning analysis and determine how space operations can meet IO requirements to assess vulnerabilities and determine follow-on requirements.
- Monitor satellite system operations in the area of C2 routing.

Assistant Chief of Staff, G-4 (Logistics)

F-25. The ACOS G-4 is the principal staff officer for all matters concerning combat service support (CSS) operations. IO-related responsibilities of the G-4 are—

- Coordinate with the ACOS G-7 on IO matters.
- Daily conduct of CSS to IO.
- Ensure IO resources are included on the combat service support control system (CSSCS) baseline resources item list and the commander's track item list.
- Provide IO CSS per priorities and requirements.
- Monitor the CSS operations of IO missions and assets.
- Track the operational readiness of IO elements and equipment.
- Provides CSS stability/capability/vulnerability input to the IO estimate and COA analyses.
- Recommend allocation of IO operational resources.
- Serve as focal point for requests for IO CSS operations.
- Serve as either a witting or unwitting participant in MD operations.
- Analyze CSS factors that influence MD operations.
- Provide CSS support to MD operations.
- Advise the DWG on how MD operations will affect CSS personnel and equipment.
- Provide a representative to the IO cell.
- Provide IO instruction in the service support annex.

Assistant Chief of Staff, G-5 (Civil-Military Operations)

F-26. The G-5 is the principal staff officer for all matters concerning civil military operations (CMO). He evaluates civil considerations within missions and identifies civil centers of gravity. IO-related responsibilities of the G-5 are—

- Coordinate with the ACOS G-7 for IO matters.
- Provide a G-5 representative to the IO cell.
- Provide IO instructions in the CMO annex.
- Conduct CMO that support IO.
- Interface between civil and military support to IO.
- Identify and procure civilian resources to support IO missions.
- Act as either a witting or unwitting participant in MD operations.
- Advise the MDO of implications of MD operations on CMO activities.
- Coordinate with the G-7 and PSYOP officer on trends in public opinion.
- Coordinate with the G-7, PAO, and PSYOP officer to ensure disseminated information is not contradictory.

Assistant Chief of Staff, G-6 (Command, Control, Communications, and Computer Operations)

F-27. The ACOS G-6 is the principal staff officer for command, control, communications, and computer operations (C4OPS) matters; network

operations (NETOPS); and IM. The IO cell includes a G-6 representative. IO-related responsibilities of the G-6 are—

- Coordinate with the G-7 on IO matters.
- Coordinate IM with and provide IM data to the G-3.
- Provide a representative to the IO cell.
- Provide IO instructions in the C4 OPS annex.
- Direct the actions of subordinate NETOPS and IM staff elements.
- Coordinate NETOPS and IM support of ISR with the G-2.
- Coordinate with the ACERT for antivirus software and threat analysis/advisories, after receiving notification of its support from the G-3.
- Coordinate with the RCERT for network intrusion devices, information, approved systems, and software, after receiving notification of its support from the G-3.

F-28. The NETOPS officer integrates mission information applications with INFOSYS and communications and computer operations of the warfighting information network. The NETOPS components are—

- **Network management**. Network management provides commanders with the ability to review and manage their networks to support ongoing IO and to adjust or reallocate network capabilities.
- **Information dissemination management**. Information dissemination management is the capability to provide a managed flow of RI based on the command's missions.
- **Information assurance**. IA includes issuing plans, orders, and polices that minimize the vulnerabilities of information, INFOSYS, and networks consistent with the defense-in-depth concept. Its goal is to protect and defend INFOSYS and networks against exploitation, degradation, and denial of services. IA responsibilities of the G-6 include IA management and CND functions.

F-29. Within corps and divisions, the G-6/IA manager supervises the IA network manager and oversees actions of subordinate unit IA security officers.

Personal Staff Officers

F-30. Personal staff officers work under the immediate control of, and have direct access to, the commander. The commander establishes guidelines or gives guidance on when a personal staff officer informs or coordinates with the COS (XO) or other staff members. The following personal staff officers have IO responsibilities.

F-31. **Public Affairs Officer.** The PAO is responsible for understanding and fulfilling the information needs of soldiers, the Army community, and the public. IO-related responsibilities are—

- Coordinate with the ACOS G-7 on public affairs (PA) issues affecting IO matters.
- Provide a PA representative to the IO cell.
- Include IO instructions in the PA annex.
- Coordinate with the PSYOP officer/NCO and G-5 to ensure PSYOP, CMO, and PA activities are not disseminating contradictory information.

- Work closely with the G-5 and other agencies to ensure an integrated strategy and a unified effort to communicate the Army's perspective and to favorably portray tactical and operational objectives.
- Act as an informed observer of the MD plan and the timetables of specific MD task executions.
- Shape the nature and angle of planned media visits to Army units that support MD plan objectives without violating policies that guide PA operations.
- Advise the DWG of the implications of the MD operation on PA operations.

F-32. **Staff Judge Advocate.** The staff judge advocate (SJA) is the commander's personal legal advisor. The SJA advises the G-3 and the G-7 on legal aspects of IO. IO-related responsibilities are—

- Advise the G-7 on the legality of IO actions being considered during planning.
- Include IO instructions in the legal appendix to the service support annex.
- Provide an SJA representative to the IO cell.
- Provide legal advice on IO rules of engagement (ROE).
- Review IO plans, policies, directives, and ROE issued by the command to ensure their consistency with DOD Directive 5100.77 and the law of war.
- Ensuring that IO law of war training and dissemination programs are consistent with DOD Directive 5100.77 and the law of war obligations of the US.
- Act as a witting participant in all MD operations.
- Advise the DWG on the legality of MD operations and the possible implications of treaty obligations and international agreements on it.

BRIGADE INFORMATION OPERATIONS RESPONSIBILITIES

F-33. There are three types of maneuver brigades: the Stryker brigade combat team (SBCT), the Army National Guard enhanced brigade, and the divisional maneuver brigade. Each has different IO capabilities.

STRYKER BRIGADE COMBAT TEAM

F-34. The Stryker brigade combat team (SBCT) includes an S-7 section, which contains an operational law team. The SBCT signal company includes a NETOPS section.

F-35. The SBCT S-7 section plans and synchronizes IO. It uses the same tactics, techniques and procedures as division and corps G-7 sections and IO cells. The S-7 includes IO, CMO, PSYOP, and EA planners. The brigade operational law team is also part of the S-7 and also serves as the SBCT's legal team. The S-7 can request augmentation of IO elements/related activities. Augmentation broadens the range of effects available to the SBCT, particularly during smaller-scale contingency operations. The IO cell has reachback capability.

F-36. The SBCT signal company NETOPS section conducts limited IA and CND functions, in coordination with the S-6 and the S-7. The NETOPS section consists of the network management, and CND teams. These teams execute installation, operation, maintenance, and limited IA and CND for the SBCT's information network. (See FM 3-31.21; FM 6-02.2; FM 6-20-40.)

F-37. The S-7 has staff responsibility for IO for the SBCT. The S-7 has the following duties:

- Advise the commander on IO and the status of friendly, neutral, and adversary IO system capabilities and limitations.
- Integrate IO into planning.
- Write the IO annex.
- Synchronize the conduct of IO.
- Oversee staff coordination for IO support from higher headquarters.
- Maintain a current IO estimate.
- Integrate IO into the targeting process.
- Nominate IO-related targets.
- Coordinate IO-related targets with higher headquarters.
- Advise fires and effects coordination cell (FECC) and S-3 on MD opportunities and capabilities.

ARMY NATIONAL GUARD ENHANCED SEPARATE BRIGADE

F-38. Since Army National Guard enhanced separate brigades can be directly subordinate to a corps; they have S-7 assigned. The enhanced separate brigade S-7 has the following duties:

- Planning the brigade IO effort.
- Assisting in developing of target lists, estimates, and assessments.
- Directing, managing, and controlling all IO assets and performing all IO tasks.
- Recommending IO priorities.
- Coordinating defensive IO with the S-2, S-3, and the S-6.
- Coordinating offensive IO with the S-2, S-3, and fire support element.

DIVISIONAL MANEUVER BRIGADE

F-39. Normally, divisions do not require subordinate maneuver brigades to plan and execute IO, but they may require brigades to accomplish IO-related tasks. Maneuver brigades normally conduct limited defensive IO. However, maneuver brigades may be tasked to perform certain actions at specific times as a part of their parent division or corps IO.

F-40. There is no IO staff section in divisional maneuver brigades. The brigade staff assumes IO responsibilities. The executive officer is the coordinator for IO within the brigade. The following are IO-related staff duties:

- The S-2 conducts physical security operations and executes counterintelligence operations.
- The S-3 conducts OPSEC operations and executes counterdeception operations.

- The S-3 is responsible for directing (per the commander's guidance) and monitoring PSYOP, and ensures that attached PSYOP teams support brigade and division PSYOP plans.
- The S-5, per the commander's guidance, monitors CMO and ensures that attached civil affairs teams support brigade and division civil affairs missions.
- The S-6 is responsible for IA in the brigade and in attached units.
- The fire support officer plans and executes IO-related physical destruction targets.

When a brigade is detached from the division, a division IO staff officer is normally attached to the brigade headquarters.

ARMY SERVICE COMPONENT COMMAND INFORMATION OPERATIONS RESPONSIBILITIES

F-41. The ACOS G-7/deputy chief of staff for information operations (DCSIO) of an ASCC has coordinating staff responsibility for IO. The G-7/DCSIO section includes a current operations division, plans division, and a PSYOP division. (IO at the operational level of war will be addressed in FM 3-93.)

F-42. The G-7/DCSIO integrates offensive and defensive IO. The G-7/DCSIO coordinates the use of assigned and supporting capabilities offensively to affect adversary and influence others' decisionmaking processes, information and INFOSYS. Defensively, the section integrates and coordinates policies and procedures, operations, personnel, and technology to protect and defend information and INFOSYS.

F-43. The G-7/DCSIO provides support to the early entry tactical operations center by forming an IO cell. The IO cell provides IO assessment of initial intheater needs of the ASCC. IO personnel form the nucleus of this cell and return to the IO section when the ASCC headquarters deploys. The G-7/DCSIO provides representatives to the JTF IO cell.

CURRENT OPERATIONS DIVISION

F-44. The current operations division accomplishes the following:

- Maintains the current IO estimate.
- Prepares IO input to FRAGOs.
- Recommends priorities for allocating critical command resources to support the IO mission, IO concept of support, IO objectives, and IO tasks.
- Recommends task organization and missions for subordinate IO-capable units to the G-3.
- Coordinates all aspects of IO, including other Service and multinational IO capabilities, with operational maneuver and operational fires.

PLANS DIVISION

F-45. The plans division integrates IO into the command's planning process. In addition to the IO duties for tactical-level planning, the plans division accomplishes the following:

- Plan operational-level OPSEC to protect the integrity of the theater military strategy and campaign plan.
- Plans and assesses MD operations to manipulate enemy operational-level commanders' perceptions and expectations and conceal friendly actions. Prepare operational-level electronic and physical deception means to support joint force campaigns.
- Prepares the IO annex.

PSYCHOLOGICAL OPERATIONS DIVISION

F-46. The PSYOP division provides staff supervision, planning, and policy recommendations on PSYOP. The PSYOP division has the following duties:

- Provide the commander with planning and policy recommendations concerning PSYOP against neutral or hostile audiences.
- Ensure coordinated efforts among PSYOP units so that their operations complement other planned operations.
- Plan for use of PSYOP assessment teams when tasked by the combatant commander (see JP 5-53).
- Coordinate and determine requirements for assigned and attached PSYOP organizations.

ECHELONS ABOVE ARMY SERVICE COMPONENT COMMAND INFORMATION OPERATIONS CAPABILITIES

F-47. Operational- and-tactical level headquarters have various IO responsibilities as discussed above. The Army echelons above ASCC to include the following can be tasked by the Army G-3 to provide support to operational- and tactical-level units.

SPACE AND MISSILE DEFENSE COMMAND

F-48. US Army Space and Missile Defense Command (SMDC) is the Army service component command of United States Strategic Command (STRATCOM) and provides Army support to STRATCOM's DOD-wide CNA/CND missions.

- SMDC synchronizes CND efforts in support of STRATCOM with Army-G-3-specified, Army-wide operational requirements and priorities.
- SMDC provides direction regarding participation in joint training exercises to 1st IOC (L) for CNA and the United States Army Network Enterprise Technology Command (NETCOM)/9th Army Signal Command for CND.

1ST INFORMATION OPERATIONS COMMAND (LAND)

F-49. Upon tasking by Army G-3, 1st IOC (L) assists, with priority to ASCCs, commanders in conducting (planning, preparing, executing, and assessing) information operations. It coordinates with joint and multinational commands, other Services, and governmental and nongovernmental agencies and organizations. ASCCs, corps, and divisions, submit requests for support through operational channels in three major areas: field support, computer emergency response, and vulnerability assessment. 1st IOC (L) can receive

reinforcement from both the Army National Guard and the Army Reserve to meet peacetime and contingency IO requirements for the Army. 1st IOC (L) command relationship are—

- 1st IOC (L) is under the operational control (OPCON) of the Army G-3.
- 1st IOC (L) is under administrative control (ADCON) of United States Army Intelligence and Security Command (INSCOM).

1st IOC (L) has the following capabilities.

Field Support Teams

F-50. Mission-tailored field support teams (FSTs) are normally the first to deploy in response to a request for IO support. FSTs provide direct support to the Army commanders of the combatant commands, designated land component commanders and ARFOR commanders of JTFs, and corps and divisions as requested. For long duration missions, FSTs deploy in an attached (less administrative) status and become part of the supported command's IO cell. They reinforce the supported command's IO efforts.

F-51. An FST, normally commanded by a field grade officer, consists of personnel with the skills and experience in conducting IO on a 24-hour-a-day basis. An FST may contain civilians and contractors. It is task-organized with other 1st IOC (L) capabilities based on such factors as mission, time-phased force and deployment data (TPFDD), funding, the supported commander's requirements and desires, and theater restrictions. A deployed FST has the following capabilities:

- Assist the G-7 through the IO-cell.
- Provide full spectrum IO analysis and support.
- Support development of plans and orders.
- Assist in planning and synchronizing IO asset employment.
- Assist in development of target lists, estimates, and assessments.
- Monitor and assess current operations and significant events for IO implications.

Army Computer Emergency Response Team

F-52. The ACERT is part of the Computer Network Operations Division. The ACERT deters, detects, coordinates, responds, and reports Army INFOSYS security incidents. The ACERT leverages and integrates intelligence support and network and system management capabilities into a unified defensive IO effort. The ACERT, operating around-the-clock, is the Department of the Army single point of contact for reporting INFOSYS security incidents and vulnerabilities, and is responsible to Headquarters, Department of the Army for coordinating an appropriate response to incidents. The ACERT is also the Army agency that exchanges reports of computer incidents and intrusions with other Service, joint, and national agencies and activities.

F-53. When tasked by the Army G-3, the ACERT dispatches personnel to assist commanders, information security managers, and system administrators by providing technical support in dealing with computer incidents and intrusions. ACERT assistance includes post-attack system restoration when required. The ACERT is the functional manager for IA tools and maintains a repository of security tools.

Information Operations Vulnerability Assessment Teams

F-54. 1st IOC (L) provides information operations vulnerability assessment teams (IOVATs), to enhance Army force protection through the assessment of a commander's ability to incorporate defensive IO into peacetime operations, operational and contingency missions, training, and exercises. Through its IOVATs, 1st IOC (L) provides focused, tailored, threat-based IO vulnerability assessment support and an adversarial capability to Army commands and the Army acquisition community.

F-55. The IOVATs contribute to force protection and IA by conducting vulnerability analyses and then recommending defensive IO countermeasures to mitigate vulnerabilities. IOVATs specialize in assessing the following areas:

- Computer telecommunications networks.
- OPSEC, communications security (COMSEC), and computer security (COMPUSEC) programs.
- EW, PSYOP, civil affairs, and PA planning and targeting.
- Decisionmaking processes.
- Data and infrastructure.

F-56. When tasked by the Army G-3, an IOVAT deploys to assess and identify vulnerabilities across the full spectrum of IO and the command's specific INFOSYS. IOVATs accomplish their missions by deploying to unit garrison, exercise, and operational areas. The teams assist units in the mitigation of command vulnerabilities to enhance force protection and IA, introducing efficiencies to enhance the command's OPSEC posture in an information-rich, digitized environment. Teams are each normally led by a field-grade officer, who coordinates directly with the commander and staff of the assessed unit.

Vulnerability Assessment Blue Teams

F-57. 1st IOC (L), vulnerability assessment blue teams, in coordination with the supported unit's staff, conduct IO force protection assessments that focus on networks and information flow within the command. Teams assimilate information to identify existing or potential vulnerabilities, estimate the level of risk, and recommend measures to diminish or eliminate that risk. Assessments consider all IO elements, unless the assessed unit's commander requests otherwise. Normally, an assessment will also include analysis of the unit's information flow infrastructure and decisionmaking process to identify choke points or potential conflicts within the command's C2 system.

F-58. The assessment process includes interviews and reviews of INFOSYS, documentation, training status, security policies, and procedures. Blue teams also assess unit vulnerabilities to adversary/threat intelligence, CNA or CNE, deception, EW/signals intelligence, and perception management (propaganda, PSYOP) activities. Teams bring the technical and nontechnical tools and expertise necessary to assess, analyze risk, and assist with the means to mitigate or eliminate vulnerabilities within the command. If requested, a team can conduct information systems security monitoring (ISSM) during the assessment.

Vulnerability Assessment Red Teams

F-59. 1st IOC (L) vulnerability assessment red teams emulate adversarial capabilities targeted against a unit's information, INFOSYS, and C2 system, and decisionmaking process. Red team missions have a dual purpose: strengthen unit readiness, and verify the effectiveness of countermeasures applied by the unit and blue teams. Red team operations are designed to provide realistic training and detailed feedback needed to strengthen a unit's defensive IO posture. The scope of red team operations, however, is limited by public law and Army policy. In addition, the assessed unit's commander may impose operational limitations. The more permissive and open the ROE, the more extensive and valuable the red team's observations and recommendations.

The Army Reprogramming Analysis Team–Threat Analysis

F-60. The Army Reprogramming Analysis Team–Threat Analysis (ARAT-TA) supports warfighters and combat/materiel developers. It identifies and reports changes in worldwide signature information that may require the rapid reprogramming of Army target sensing systems. Army target sensing systems are those radar warning, surveillance, self-protection systems and smart munitions that incorporate software algorithms to identify threat systems based upon embedded reprogrammed threat parameter data. Examples include smart/brilliant munitions, sensors, processors, and aviation electronic combat survivability equipment. The ARAT-TA provides assistance that supports Army aviation survivability.

Current Operations Center

F-61. The current operations center is the focal point of 1st IOC (L) activities. It includes an operations capability, an IO intelligence support capability, and a robust communications capability.

F-62. The current operations center provides support to 1st IOC (L)'s deployed teams and the supported commands. The teams support through the concept of split-based operations. Tailored analytical products can be produced and provided to meet a deployed team's immediate needs.

F-63. The intelligence support element also provides support to the initial planning requirements of teams preparing for deployment. The operations element maintains the status of internal day-to-day 1st IOC (L) activities and of the current situation of all deployed teams, facilitating responsive IO support to supported commands. The robust communication capability facilitates the integration of all IO support.

Computer Network Operations

F-64. The 1st IOC (L) is under tactical control (TACON) of SMDC for CNA. (See definition at paragraph 2-31).

F-65. The relationship between 1st IOC (L) and the Army G-3 and remains unchanged. Army G-3 continues to directly task the 1st IOC (L) for support to other Army service component commands and major Army commands.

US ARMY INTELLIGENCE AND SECURITY COMMAND

F-66. INSCOM's IO capabilities focuses around the Information Dominance Center (IDC). The IDC integrates intelligence operations and IO to support ASCCs and other Army forces through its deployed teams. As an integrating intelligence center, the IDC provides intelligence support to counterintelligence, CNA, and CND activities.

F-67. The IDC supports Army commands and units worldwide through G-2 channels for intelligence-reach operations. The IDC can provide tailored intelligence products to the field to meet their operational requirements on a quick response basis. The IDC monitors potential trouble spots, preparing to support contingency operations with intelligence related products. The IDC continues to explore new analytical technologies and emerging concepts to support Army warfighters.

F-68. INSCOM's Cyber Warfare Center (CWC), 1st IOC (L)'s ACERT, and NETCOM's Army Network Operations and Security Center (ANOSC) normally co-locate with the IDC. The IDC also provides a liaison link to CND and CNA operations of the combined CWC, ACERT, and ANOSC.

US ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH ARMY SIGNAL COMMAND

F-69. NETCOM/9th Army Signal Command supports SMDC by defending the Army Enterprise Infostructure. This task includes the following responsibilities:

- Exercise technical control and configuration management authority for Army networks and systems.
- Retain the authority to deny connectivity to Army networks in defense of Army or other DOD operations (after coordination with the required Army or DOD authorities and the Army G-3 or his designated representative).

F-70. The ANOSC is the Army's central NETOPS control facility for its portion of the Global Information Grid (GIG). (See FM 6-02.71.) The ANOSC provides worldwide operational and technical support to the Army's portion of the GIG across the strategic and operational levels, and into the tactical level. The ANOSC gives the Army the worldwide capability to provide a consolidated, coordinated, protected, and properly configured information network and systems operation.

F-71. Examples of the mission of the ANOSC include—

- Interfacing and sharing data with the Defense Information Systems Agency's Global Network Operations and Security Center to ensure that support to networks and INFOSYS using the GIG's backbone is responsive and configured to meet Army operational requirements.
- Performing all NETOPS activities, functions, and tasks for Army split-base operations and sustaining-base INFOSYS, enabling full spectrum dominance.
- Providing NETOPS support for assigned Army IO systems.

- Coordinating with the ACERT to ensure protective CND procedures are in place.

F-72. SMDC has tactical control (TACON) of the ANOSC for CND. The ANOSC has TACON of the ACERT for CND.

Appendix G

Example of IO-Focused Fragmentary Order

This appendix contains an example of a fragmentary order for a support operation in a combat zone. It continues the scenario begun in appendix B.

G-1. Several hours after XXI Corps and Army of San Anglos (ASA) forces launched their attack, Rendovan saboteurs detonated a bomb that destroyed a fertilizer plant near the city of San Jacinto, located in eastern San Anglos (see figure B-1, page B-2). The government of San Anglos requested XXI Corps to help them maintain order until San Anglos civil and military authorities could reassert control. They also requested help in cleaning up contamination from the blast and treating injured civilians.

G-2. The XXI Corps staff has prepared a contingency plan, OPLAN Provider that addresses this sort of situation. OPLAN Provider tasks the corps troops, including the tactical combat force, to prepare their own implementation plans. Upon being notified of the attack, the XXI Corps deputy commander for support directed execution of OPLAN Provider. The corps command post issued the fragmentary order in figure G-1 to all units in Assembly Areas Jackson and Stewart.

Copy___of___copies
Headquarters, XXI Corps
DTG

FRAGMENTARY ORDER 03-01-01

References: XXI Corps OPORD 03-01
XXI Corps OPLAN Provider (Emergency Assistance)

Task Organization: TF Provider

TF 2-4 IN	361 PSYOP Co.
122 CM Bn.	102 MI Bn. (DS)
212 MP Co.	404 BCT (DS)
301 MP Co.	702 Support Bn. (DS)

1. **Situation**: At 0900 DTG, an unknown saboteur detonated a large bomb at the fertilizer plant outside San Jacinto, vicinity [grid]. The blast destroyed the plant and produced a hazardous area 2 kilometers in diameter. The government of San Anglos has requested assistance in consequence management of the incident.

a. **Enemy Forces**.

Figure G-1. XXI Corps Fragmentary Order

(1) Rendovan special purpose forces (SPF) continue to operate in the eastern San Anglos. They are attempting to insert themselves into NGOs and within the community of San Jacinto to provide cover for intelligence collection missions and to disrupt the efforts of US and ASA forces. SPF sniper teams may be the biggest threat to US soldiers, senior civilian advisors, and political figures. SPF may conduct direct action against soft targets, such as squad-size elements of US soldiers or unprotected C2 nodes. SPF aim is to cause widespread panic and to undermine US forces morale.

(2) Members of the Rendovan Liberation Front (RLF) will continue efforts to organize local insurgent groups. RLF will initiate demonstrations against US-led operations. RLF will attempt to turn demonstrations violent in order for local media to capture film of US soldiers manhandling civilians.

b. **Friendly Forces**.

(1) **XXI Corps**. No change.

(2) **Army of San Anglos (ASA)**.

(a) ASA decisive operation is attack to expel Tiger Corps from San Anglos.

(b) A San Anglos task force consisting of civilian and military elements is assembling vicinity Harar [grid]. It anticipates taking control of San Jacinto and the surrounding area within 48 hours.

(3) San Jacinto civil authorities and police force are intact.

2. **Mission**. TF Provider deploys to San Jacinto to provide support to civil authorities and clean up contamination from destroyed fertilizer plant. TF Provider establishes a class I food distribution point to support NGO assistance efforts; provides medical support to local medical facilities; prevents/controls civil unrest by supporting the San Jacinto police force; and transfers authority to ASA task force upon its arrival (NLT D + 4).

3. **Execution**.

Intent. This is a critical event. Its success is necessary to maintain the faith of the local populace in the San Anglos government. Move quickly to render aid while maintaining the security of the force.

a. **Concept of operations**.

(1) **Tasks to be executed**.

(a) Secure area/protect the force.

(b) Distribute/provide food, water, and emergency medical services.

(c) Maintain public order and safety, to include crowd control.

(d) Establish liaison with local authorities and NGOs.

(e) Be prepared to protect NGO food convoys to prevent looting.

(f) Clean up contamination from destroyed fertilizer plant.

Figure G-1. XXI Corps Fragmentary Order (continued)

(2) **This operation will take place in five phases**.

(a) **Phase I—Alert, marshal and deploy**. TF 2-14 IN assembles TF Provider and begins preparation for movement. Maintains communications with XXI Corps CP. Coordinates with CMOC for most current civil situation and area orientation.

(b) **Phase II—Occupy Intermediate Staging Area and Assess Situation**. Move by ground or air to an AA Provider, vicinity [grid], near the crisis area and establish security. Establish liaison with the local government and HN/NGO support agencies. Recon AO San Jacinto and refine the plan for support.

(c) **Phase III—Secure AO San Jacinto**. Occupy distribution sites and establish security. Supplies are staged out of AA Provider. Conduct aggressive patrolling to expand secure areas in the town. Establish additional distribution nodes as necessary. Incorporate available HN/NGO relief operations. Encourage host nation involvement in planning, coordination, and execution to exhibit positive relations. Protect resources from weather damage and theft. Conduct continuous force protection.

(d) **Phase IV—Maintain Order and Distribute Aid**. Maintain order in AO San Jacinto. Distribute supplies, support, and MA technical assistance and services to local population. Monitor NGO/HN relief operations, assess vulnerabilities, and maintain force protection.

(e) **Phase V—Transfer Authority/Support and Redeploy**. Transfer operations to ASA task force NLT is D + 4. Specific handover criteria include—

(i) All civilian casualties recurring from incident are treated and under medical care of local doctors/medical facilities.

(ii) Class I distribution point established and capable of distributing required number of meals per day. NGOs and/or local officials are capable of continuing distribution

(iii) No looting, demonstrations, or other forms of civil unrest occurring.

(iv) Upon handover, TF Provider redeploys to parent unit for recovery and prepares to reassume TCF mission.

b. **Tasks to subordinate units.**

(1) **TF 2-41 IN.**

(a) Command and control TF Provider.

(b) Designate leadership for security, transportation, and sustainment forces.

(c) Secure AA Provider NLT 2100 D-day.

(d) Be prepared to receive aerial delivery of foodstuffs at AA Provider NLT 0600 D + 1.

(e) Initiate liaison with local officials NLT 1200 D-day.

(f) Be prepared to receive augmentation personnel via helicopter NLT 1200 D-day.

Figure G-1. XXI Corps Fragmentary Order (continued)

(g) Coordinate HN/NGO support with the G-5.

(h) Coordinate ROE with SJA.

(i) Coordinate with G-5 to identify local populace needs in AO San Jacinto.

(2) **361st PSYOP Co.** Conduct aerial loudspeaker, leaflet, and broadcast missions. Script instructs citizens of San Jacinto to stay away from fertilizer plant and provides locations of aid distribution points and medical aid stations. Script instructs citizens to report any information regarding Rendovan activity to local officials.

(3) **2d MP Co. and 301st MP Co.**

(a) Provide forces to escort TF Provider to AA Provider.

(b) Secure AA Provider.

(c) On order, escort NGO food convoys within AO San Jacinto.

(4) **102d MI Bn. (DS)**.

(a) Assess local national sentiment for US operations.

(b) Provide a team to conduct force protection operations. Available for aerial movement from DSA Zinc NLT DTG.

(c) Conduct liaison with HN police forces.

(d) Provide threat and vulnerability assessment throughout the operation.

(5) **404th BCT. (DS)**.

(a) Provide helicopters for movement of 25 tons of food. PZ is [grid]. LZ is AA Provider. Deliver food to LZ NLT DTG.

(b) Provide lift support as required to NGO officials, providing they sign a legitimate-target waiver.

(c) Be prepared to provide precision fires to

(6) **702 Support Bn. (DS)**.

(a) Move initial logistic element by aerial movement from DSA Zinc NLT DTG. Ground element departs NLT DTG to AA Provider.

(b) Provide CSS to TF Provider.

(c) Provide class I and water sufficient for 3,500 civilians.

(d) Provide occupational health support to San Jacinto to assess hazard area.

(e) Provide medical supplies and technical assistance.

(f) On order, operate LZ to receive supplies via rotary wing.

(7) **122d Chemical Bn**. Clean up contamination from destroyed fertilizer plant, vicinity San Jacinto.

c. **Tasks to Staff**

Figure G-1. XXI Corps Fragmentary Order (continued)

(1) G-5/CMOC.

(a) Co-locate with HQ, TF 2-4 IN.

(b) Identify and coordinate with local governmental officials.

(c) Provide liaison to local government.

(d) Identify and coordinate for available HN support.

(e) Coordinate, via CMOC, support for NGOs.

(2) **PAO**. Produce a press release that emphasizes the following points:

(a) The destruction of the fertilizer plant in San Jacinto was a terrorist act committed by the RLF.

(b) The destruction of the fertilizer plant had absolutely no military value and was solely done for the purpose of creating civilian casualties.

(c) TF Provider forces moved into AO San Jacinto to minimize civilian casualties.

(d) TF Provider forces, together with NGOs and local authorities, are establishing food distribution points.

(e) TF Provider is providing medical support and security forces to assist local authorities in San Jacinto.

(3) **Surgeon**. Coordinate with Corps medical logistics battalion for aerial delivery of 10 burn kits, 500 units O-negative blood, and 10 surgical kits.

d. **Coordinating Instructions**.

(1) **Talking points**. The following talking points are guidelines for all TF Provider soldiers when referring to the act of sabotage on the San Jacinto fertilizer plant. These talking points serve as guidelines should soldiers find themselves talking to the press or civilian organizations. These points should not be read verbatim but serve as a guide to information that is factual and known at this point. Refer requests for any further information to the PAO.

(a) The terrorist group known as the Rendovan Liberation Front (RLF) conducted the attack on the fertilizer plant.

(b) The fertilizer plant at San Jacinto was destroyed, releasing toxic chemical gases into the air in the vicinity of the plant.

(c) The exact numbers of civilians killed and how many were left homeless is still being determined but the damage around the plant was extensive.

(d) US forces are working as part of a coordinated effort with the mayor of San Jacinto and international aid organizations to render the maximum amount of aid to the civilian casualties of this terrorist attack.

(e) We cannot comment on the exact nature or location of any support being provided. Obtain further information on specific US involvement from the PAO.

Figure G-1. XXI Corps Fragmentary Order (continued)

(f) We extend our fullest sympathies and support to the San Jacinto people who are the victims of this act of terrorism.

(2) **Toxic Chemical Hazard**. Primary toxic chemical hazards include dichloroaniline, chloropyridinyls, and benzoic acid. Characteristics, protective measures, and first aid include—

(a) Inhalation and contact hazard.

(b) Combustible when heated.

(c) Runoff is toxic and corrosive. Use water to cool containers. Do not get water inside containers.

(d) Move casualties to area with fresh air. Provide oxygen.

(e) Do not use direct mouth-to-mouth due to transfer of hazard. Isolate contaminated clothing. Avoid spreading contamination to unaffected skin.

(f) Flush eyes and skin with water for 20 minutes if directly contaminated.

(3) **CCIR**.

(a) Size and location of enemy forces in area.

(b) Number of civilian casualties by type (urgent-surgical, urgent, priority, routine) and age/gender/obstetrics.

(c) Location and capabilities of HN support facilities in AO San Jacinto.

(d) Location and capabilities of NGO in area.

(e) Class I, VIII, and blood availability from HN.

(f) Was the fertilizer plant destroyed by a WMD or conventional explosive?

(g) HN lift/evacuation assets in area.

(h) What religious support is available in area?

(4) Coordinate with XXI Corps Finance for needs best met by procurement.

4. **Service Support**. 702d Support Bn. is TF Provider CSS HQ.

5. **Command and Signal**.

a. **Command**.

(1) Cdr., TF 2-14 is Cdr., TF Provider.

(2) XXI Corps CP controls operation.

b. **Signal**. No change.

ACKNOWLEDGE:

SMITH
LTG

Figure G-1. XXI Corps Fragmentary Order (continued)

Glossary

The glossary lists acronyms and terms with Army or joint definitions, and other selected terms. Where Army and joint definitions are different, *(Army)* follows the term. Terms for which FM 3-13 is the proponent manual (the authority) are marked with an asterisk (*). The proponent manual for other terms is listed in parentheses after the definition. Terms that include *information operations* are listed under *IO*.

1st IOC (L) 1st Information Operations Command (Land)

AA assembly area

AAR after-action report

accident risk All operational risk considerations other than tactical risk. (FM 100-14)

ACE analysis and control element

ACERT Army Computer Emergency Response Team

ACR armored cavalry regiment

AD air defense

ADA air defense artillery

ADC-M assistant division commander–maneuver

ADC-S assistant division commander–support

adjustment decision During preparation and execution, the selection of a course of action that modifies the order to respond to unanticipated opportunities or threats. (FM 6-0)

administrative means *See* deception means.

adversary A person or group that is opposed to an Army force mission but is not engaging Army forces in combat operations.

AEF aerospace expeditionary force

AFFOR Air Force forces

AGM attack guidance matrix

AI air interdiction

AM amplitude modulated

ANOSC United States Army Network Operations and Security Center

AO area of operations

AOA amphibious objective area

AOR area of responsibility

AR Army regulation

ARAT-TA Army Reprogramming Analysis Team–Threat Analysis

area of interest (joint) That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. (JP 3-0)

area of responsibility (joint) The geographical area associated with a combat command within which a combatant commander has authority to plan and conduct operations. (JP 3-0)

ARFOR The senior Army headquarters and all Army forces assigned or attached to a combatant command, subordinate joint force command, joint functional command, or multinational command. (FM 3-0)

ARSPACE United States Army Space Command

ASA Army of San Anglos (scenario use only)

ASC Army Signal Command

ASCC Army service component command

assessment (Army) The continuous monitoring—throughout planning, preparation and execution—of the current situation and progress of an operation, and the evaluation of it against criteria of success to make decisions and adjustments. (FM 3-0)

ATACMS Army Tactical Missile System

battlespace (joint) 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 information environment within the operational areas and areas of interest. (JP 3-0)

BCT brigade combat team

BDA battle damage assessment

bde brigade

bn battalion

BOS battlefield operating system

BSA brigade support area

C2 command and control

C3IC coalition coordination, communications, and integration center

C4OPS command, control, communications, and computer operations

CA civil affairs

CAB	combat aviation brigade
CAC	Combined Arms Center
CAS	close air support
CCIR	commander's critical information requirements
cdr	commander
CENTCOM	United States Central Command
CG	commanding general
CHOP	change of operational control
CI	counterintelligence
CID	criminal investigation division
civil affairs	(joint) Designated active and reserve component forces and units organized, trained, and equipped specifically to conduct civil affairs activities and to support civil-military operations. (JP 3-57)
civil-military operations	(joint) The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. (JP 3-57)
CJCS	Chairman of the Joint Chiefs of Staff
CJTF	commander, joint task force
CMO	civil-military operations
CMOC	civil-military operations center
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
co	company
COA	course of action
COLISEUM	Common On-line Intelligence System for End User and Management

combat power (joint/NATO) The total means of destructive and/or disruptive force, which a military unit/force can apply against the opponent at a given time. (JP 1-02)

command and control (Army) The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Commanders perform command and control functions through a command and control system. (FM 6-0)

command and control system (Army) The arrangement of personnel, information management, procedures, and equipment and facilities essential to the commander to conduct operations. (FM 6-0)

commander's critical information requirements (Army) Elements of information required by commanders that directly affect decisionmaking and dictate the successful execution of military operations. (FM 3-0)

commander's intent (Army) A clear, concise statement of what the force must do and the conditions the force must meet to succeed with respect to the enemy, terrain, and the desired end state. (FM 3-0)

communications (joint) A method or means of conveying information of any kind from one person or place to another. (JP 6-0)

communications security (joint) The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications security includes: cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. a. cryptosecurity—The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. transmission security—the component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. emission security—the component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. physical security—The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP 3-13)

COMPUSEC computer security

computer network attack (joint) 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 specturem. 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 to destroy a computer's electronics and causing the same result is EA. (JP 1-02)

computer network defense (joint) Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. (JP 3-51)

***computer network exploitation** Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. (This definition is consistent with joint initiatives and is being staffed as a possible joint definition.)

***computer network operations** Computer network attack, computer network defense, and related computer network exploitation enabling operations. (This definition is consistent with joint initiatives and is being staffed as a possible joint definition.)

COMSEC communications security

constraint A restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action the subordinate commander has for planning. (FM 5-0)

control (Army) Within command and control, the regulation of forces and battlefield operating systems to accomplish the mission in accordance with the commander's intent. It includes collecting, processing, displaying, storing, and disseminating relevant information for creating the common operational picture, and using information, primarily by the staff, during the operations process. (FM 6-0)

COP common operational picture

COS chief of staff

counterdeception (joint) Efforts to negate, neutralize, diminish the effects of, or gain the advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (JP 3-13)

counterintelligence (joint) Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 3-13)

counterpropaganda Programs of products and actions designed to nullify propaganda or mitigate its effects. (FM 3-05.30)

CP command post

criteria of success Information requirements developed during the operations process that measure the degree of success in accomplishing the unit's

	mission. They are normally expressed as either an explicit evaluation of the present situation or forecast of the degree of mission accomplishment. (FM 6-0)
***critical asset list**	A list of intelligence, surveillance, and reconnaissance elements, and elements of the command's command and control system, whose loss or functional disruption would jeopardize mission accomplishment.
CSS	combat service support
DA	Department of the Army
DC	dislocated civilian
DCSINT	deputy chief of staff for intelligence
DCSIO	deputy chief of staff for information operations
D-day	(joint) The unnamed day on which a particular operation commences or is to commence.
***deceive**	To cause a person to believe what is not true.
deception event	(joint) A deception means executed at a specific time and location in support of a deception operation. (JP 3-58)
deception means	(joint) Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. **physical means**—Activities and resources used to convey or deny selected information to a foreign power. (Examples include military operations, including exercises, reconnaissance, training activities, and movement of forces; the use of dummy equipment and devices; tactics; bases, logistic actions, stockpiles, and repair activity; and test and evaluation activities.) b. **technical means**—Military materiel resources and their associated operating techniques used to convey or deny selected information to a foreign power through the deliberate radiation, re-radiation, alteration, absorption, or reflection of energy; the emission or suppression of chemical or biological odors; and the emission or suppression of nuclear particles. c. **administrative means**—Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 3-58)
deception objective	(joint) The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location. (JP 3-58)
deception story	(joint) A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. (JP 3-58)
deception target	(joint) The adversary decisionmaker with the authority to make the decision that will achieve the deception objective. (JP 3-58)
***deception working group**	A group tailored to bring together the special technical skills required to conduct a specific military deception operation.

***defense in depth** In information operations, the integration of the capabilities of people, operations, and technology to establish multi-layer, multi-dimension protection.

defensive information operations (Army) The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (FM 3-0)

***degrade** In information operations, using nonlethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems and informtion collection efforts or means.

denial of service Action or actions that result in the inability of an automated information system or any essential part to perform its designated mission, either by loss or degradation of operational capability.

***deny** In information operations, entails withholding information about Army force capabilities and intentions that adversaries need for effective and timely decisionmaking.

desired perception (joint) In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective. (JP 3-58)

destroy To damage a combat system so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt. (FM 3-90)

det detachment

***detect** To discover or discern the existence, presences or fact of an intrusion into information systems.

***disinformation** Information disseminated primarily by intelligence organizations or other covert agencies designed to distort information, or deceive or influence United States decisionmakers, United States forces, coalition allies, key actors, or individuals by indirect or unconventional means.

DISA Defense Information Systems Agency

DISN Defense Information Systems Network

***disrupt** In information operations, breaking or interrupting the flow of information between selected command and control nodes.

div **division**

DOD Department of Defense

DODD Department of Defense Directive

DODDIP Department of Defense Defense Intelligence Production Program

DOS Department of State

DS direct support

DSM decision support matrix

DSO deception staff officer

DTG date-time group

DWG deception working group

EA electronic attack

EAC echelons above corps

EEFI essential elements of friendly information

electromagnetic deception (joint) The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic dependent weapons, thereby, degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are: a. manipulative electromagnetic deception—Actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces; b. simulative electromagnetic deception—actions to simulate friendly, notional, or actual capabilities to mislead hostile forces; imitative electromagnetic deception—the introduction of electromagnetic energy into enemy systems that imitates enemy effusions. (JP 3-51)

electromagnetic spectrum (joint) The range of frequencies o f electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 3-13.1)

electronic attack *See* electronic warfare.

electronic protection *See* electronic warfare.

electronic warfare (joint) Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: 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. Electronic attack 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. 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. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 3-51)

electronic warfare support *See* electronic warfare.

ENCOORD engineer coordinator

enemy an individual or group engaging Army forces in combat

EP electronic protection

ES electronic warfare support

essential elements of friendly information (Army) The critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation, and therefore must be protected from enemy detection. (FM 3-0)

EW electronic warfare

EWO electronic warfare officer

execution decision The selection, during preparation and execution, of a course of action anticipated by the order. (FM 6-0)

***exploit** In information operations to gain access to adversary C2 systems to collect information or to plant false or misleading information.

FA field artillery

FARP forward arming and refueling point

***feedback** Information that reveals how the deception target is responding to the deception story and if the military deception plan is working.

FECC fires and effects coordination cell

FFIR friendly forces information requirements

***field support team** A team that provides direct support information operations to the ARFORs and joint task forces of land components of combatant commands, and corps and divisions as requested.

firmware Computer programs contained permanently in a hardware device as a read-only memory.

FLOT forward line of own troops

***forms of uncertainty** In military deception, means of shaping the deception target's perceptions. Increasing uncertainty aims to confuse the deception target. Reducing uncertainty aims to reinforce the deception target's predispositions.

FM frequency modulated

FRAGO fragmentary order

friendly forces information requirements Information the commander and staff need about the forces available for the operation. (FM 6-0)

FSE fire support element

FST field support team

FSCOORD fire support coordinator

full spectrum operations The range of operations Army forces conduct in war and military operations other than war. (FM 3-0)

G-1 assistant chief of staff, human resources

G-2 assistant chief of staff, intelligence

G-3 assistant chief of staff, operations

G-4 assistant chief of staff, logistics

G-5 assistant chief of staff, civil-military operations

G-6 assistant chief of staff, command, control, communications, and computer operations (C4OPS)

G-7 assistant chief of staff, information operations

Global Information Grid (joint) 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 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, 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. (JP 1-02)

grp group

hazard (joint) A condition with the potential to cause injury, illness or death of personnel; damage to, or loss of, equipment or property; or mission degradation. (JP 1-02)

HF high frequency

H-hour (joint) The specific hour on D-day at which a particular operation commences.

high-payoff target (joint) A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through war-gaming, that must be acquired and successfully attacked for the success of the friendly commander's mission. (JP 1-02)

high-value target (joint) A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. (JP 1-02)

HN host nation/host-nation

HPT high-payoff target

HPTL high-payoff target list

hq headquarters

HUMINT human intelligence

HVT high-value target

IA information assurance

IANM information assurance network manager

IASO information assurance security officer

ID infantry division

IDC information dominance center

IM information management

IMINT imagery intelligence

incident (joint) In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. (JP 3-13)

indicator (joint/NATO) In intelligence usage, is an item of information which reflects the intentions or capability of a potential enemy to adopt or reject a course of action. (JP 1-02)

***indicator feedback** Information that indicates whether and how the deception story is reaching the deception target.

***influence** To cause adversaries or others to behave in a manner favorable to Army forces.

INFOCON information operations conditions

information (Army) (1) In the general sense, the meaning humans assign to data. (2) In the context of the cognitive hierarchy, data that have been processed to provide further meaning. (FM 6-0)

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

information environment (joint) The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (JP 3-13)

***informational fratricide** The results of employing information operations elements in a way that causes effects in the information environment that impede the conduct of friendly operations or adversly effect friendly forces.

information management The provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decisionmaking. It uses procedures and information systems to collect, process, store, display, and disseminate information. (FM 3-0)

information operations The employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decisionmaking. (This definition supersedes the definition of information operations in FM 3-0. It is consistent with joint initiatives.)

information security (joint) The protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of services 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. (JP 3-13)

information superiority (Army) The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (FM 3-0)

information systems (Army) The equipment and facilities that collect, process, store, display and disseminate information. This includes computers—hardware and software—and communications, as well as policies and procedures for their use. (FM 3-0)

IO information operations

***IO assets** Organic, assigned and attached units with information operations capabilities.

***IO capabilities** Units or systems that support the accomplishment of information operations tasks.

***IO cell** A grouping of staff officers to synchronize IO throughout the operations process.

***IO concept of support** A clear, concise statement of where, when, and how the commander intends to focus the information element of combat power to accomplish the mission.

***IO mission statement** A short paragraph or sentence describing what the commander wants information operations to accomplish and the purpose for accomplishing it.

***IO objectives** Clearly defined, obtainable aims that the commander intends to achieve using information operations elements/related activities.

***IO resources** Information-operations-capable units not assigned or attached to the command, but whose capabilities are available to conduct information operations.

***IO tasks** Tasks developed to support accomplishment of one or more IO objectives.

IOVAT information operations vulnerability assessment team

***IO vulnerabilities** Deficiencies in protective measures that may allow an adversary to use information operations capabilities against friendly information systems or command and control systems.

***IO vulnerability assessment team** A team designed to enhance army force protection through the Army commander's ability to incorporate defensive information operations into peacetime operations, operational and contingency missions, training and exercises.

infostructure The hardware, software, and communications information technologies and associated architectures and facilities that ensure universal access, security, privacy, and reliability of Army networks. (FM 6-02.71)

IN infantry

INFOSYS information systems

INSCOM United States Army Intelligence and Security Command

intelligence (joint) (1) The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. (2) Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

intelligence preparation of the battlefield A systematic approach to analyzing the enemy and environment (for example, weather, terrain and civil considerations) in a specific geographic area. It integrates enemy doctrine with the weather, terrain, and civil considerations as they relate to the mission and the specific environment. This is done to

determine and evaluate enemy capabilities, vulnerabilities, and probable courses of actions. (FM 34-130)

IPB intelligence preparation of the battlefield

IPIP International Public Information Program

IPW interrogation, prisoner of war

IR information requirement

ISR intelligence, surveillance, and reconnaissance

JCS Joint Chiefs of Staff

JFACC joint force air component commander

JFC joint force commander

JFLCC joint force land component commander

JOA joint operations area

JP joint publication

JRA joint rear area

JSEAD joint suppression of enemy air defenses

JTF joint task force

key tasks Those tasks the force as a whole must perform, or conditions the force must meet, to achieve the end state and stated purpose of the operation. (FM 6-0)

LAN local area network

LOC line of communications

log logistic/logistics

LZ landing zone

manipulative electromagnetic deception *See* electromagnetic deception.

MARFOR Marine Corps forces

MASINT measurement and signature intelligence

MCS mobility/countermobility/survivability

MD military deception

MDMP military decisionmaking process

MDO military deception officer

MEB Marine expeditionary brigade

METT-TC A memory aid used in two contexts: (1) In the context of information management, the major subject categories into which relevant information is grouped for military operations: mission, enemy, terrain and weather, troops and support available, time available, civil considerations. (2) In the context of tactics, the major factors considered during mission analysis. (FM 6-0)

MI military intelligence

military deception (joint) Actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are 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**. 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. (JP 3-58)

***misinformation** Incorrect information from any source that is released for unknown reasons or to solicit a response or interest from a nonpolitical or nonmilitary target.

mm millimeter

MOS military occupational specialty

MP military police

MSE mobile subscriber equipment

mutual support Support that units render to each other against an enemy because of their assigned tasks, their position relative to each other and to the enemy, and their inherent capabilities. (JP 1-02)

mtg meeting

NATO North Atlantic Treaty Organization

NAVFOR Navy forces

NBC nuclear, biological, and chemical

near real-time Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP 1-02)

NETOPS network operations

network operations The collaborative, integrated management of networks, information systems, and resources that provide a common operation picture. (FM 6-02.71)

NGO nongovernmental organization

NLT not later than

nongovernmental organizations Transnational organizations of private citizens that maintain a consultative status with the Economic and Social Council of the United Nations. Nongovernmental organizations may be professional associations, foundations, multinational businesses, or simply groups with a common interest in humanitarian assistance activities (development and relief). "Nongovernmental organizations" is a term normally used by non-United States organizations. (JP 3-16) (In FM 3-13, nongovernmental organizations include private voluntary organizations.)

offensive information operations (Army) The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decisionmakers or to influence others to achieve or promote specific objectives. (FM 3-0)

operations process The activities performed during operations: plan, prepare, and execute with continuous assessment. (FM 6-0)

***operations security** (Army) A process of identifying essential elements of friendly information and subsequent analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPLAN operation plan

OPORD operation order

***opposing information** Intentional or unintentional truth-based information from any source that represents an opposing view.

OPSEC operations security

***OPSEC indicator** (Army) Friendly detectable actions and open-source information that can be intercepted or pieced together by an adversary to derive essential elements of friendly information.

***OPSEC measures** Methods and means to gain and maintain essential secrecy about essential elements of friendly information.

***OPSEC planning guidance** (Army) The blueprint for operations security planning. It defines the essential elements of friendly information, taking into account friendly and adversary goals, probable adversary knowledge, friendly deception objectives, and adversary collection capabilities. It also should outline provisional operations security measures.

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

PA public affairs

PAO public affairs officer

***perception feedback** Information that indicates whether the deception target is responding to the deception story.

perception management (joint) Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover, deception, and psychological operations. (JP 3-13)

***perceptions** Mental images the commander wants the deception target to believe are real.

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

physical means *See* deception means.

physical security (joint) That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 3-13)

planning The means by which the commander envisions a desired outcome, lays out effective ways of achieving it, and communicates to his subordinates his vision, intent, and decisions, focusing on the results he expect to achieve. (FM 3-0)

PIR priority intelligence requirement

priority intelligence requirements (joint/NATO) Those intelligence requirements for which a commander has an anticipate and stated priority in the task of planning and decisionmaking. (JP 1-02)

propaganda Any form of communications in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. (JP 3-53)

***protect** All actions taken to guard against espionage or capture of sensitive equipment and information.

psychological operations (joint) 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, individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 3-53)

PSYOP psychological operations

public affairs (joint) Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in DOD. (JP 3-61)

R&D research and development

RCERT regional computer emergency response team

real time (joint) Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. (JP 1-02)

REC radio electronic combat (scenario use only)

reconnaissance (joint) The mission undertaken to obtain by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (JP 1-02)

relevant information All information of importance to commanders and staffs in the exercise of command and control. (FM 3-0)

***respond** In informations operations is to act positively to an adversary's IO attack or intrusion.

***restore** To bring information systems back to their original state.

RFI request for information

RLF Rendovan Liberation Front (scenario use only)

RI relevant information

risk management (joint) The process of identifying, assessing, and controlling risk arising from operational factors, and making decisions that balance risk cost with mission benefits. (JP 1-02)

ROE rules of engagement

RTOC rear tactical operations center

SA systems administrator

SBCT Stryker brigade combat team

SCI sensitive compartmented information

SEAD suppression of enemy air defense

SED simulative electronic deception

SEP signals intelligence end products

SIGINT signals intelligence

situational understanding The product of applying analysis and judgment to the common operational picture to determine the relationships among the factors of METT-TC. (FM 3-0)

situation template (joint) A depiction of assumed adversary dispositions, based on adversary doctrine and the effects of the battlespace if the adversary should adopt a particular course of action. In effect, the situation templates are the doctrinal templates depicting a particular operation modified to account for the effects of the battlespace environment and the adversary's current situation (training and experience levels, logistic status, losses, dispositions). Normally, the situation template depicts adversary units two levels of command below the friendly force, as well as the expected locations of high-value targets. Situation templates use time-phase lines to indicate movement of forces and the expected flow of the operation. Usually the situation template depicts a critical point in the course of action. Situation templates are one part of an adversary course of action model. Models may contain more than one situation template.

SJA staff judge advocate

SMDC US Army Space and Missile Defense Command

SME subject matter expert

SOCCE special operations command and control element

SOCOM United States Army Special Operations Command

SOCOORD special operations coordinator

SOP standing operating procedure

SPF special purpose forces (scenario use only)

STRATCOM United States Strategic Command

***subordinate deception objective** A restatement of the deception objective in terms that reflect the deception target's point of view.

***supporting perceptions** Mental images that enhance the likelihood that the deception target will form the desired perceptions and accept them as true.

surveillance (joint) The systematic observation of aerospace, surface or subsurface areas, places, persons, or things by visual, aural, electronic, photographic or other means. (JP 1-02)

tac	tactical (used with CP [command post])
TACON	tactical control
tactical combat force	(joint) A combat unit, with appropriate combat support and combat service support assets, that is assigned the mission of defeating Level III threats. (JP 1-02)
tactical risk	Risk concerned associated with hazards that exist because of the presence of either the enemy or an adversary. (FM 100-14)
TACWAN	tactical wide area network
TAD	target acquisition detachment
TBD	to be determined
TCF	tactical combat force
technical means	*See* deception means.
tempo	The rate of military action. (FM 3-0)
TF	task force
tgt	target/targeting
tm	team
TOT	time on target
TPFDD	time-phased force and deployment data
TSM	target synchronization matrix
TSS	target selection standards
TTP	tactics, techniques, and procedures
TVA	target value analysis
UAV	unmanned aerial vehicle
UAV-SR	unmanned aerial vehicle–short range
***unwitting actor**	An individual participating in the conduct of a military deception operation without personal knowledge of the facts of the deception.
US	United States
USAID	United States Agency for International Development
USAJFKSWCS	United States Army John Fitzgerald Kennedy Special Warfare Center and School
USC	United States Code
USIA	United States Information Agency
VA	vulnerability assessment
VAP	vulnerability assessment program
VAT	vulnerability assessment team
VHF	very high frequency

WARNO	warning order
***witting actor**	An individual participating in the conduct of a military deception operation who is fully aware of the facts of the deception.
wpns	weapons
WTEM	weather, terrain and environmental monitoring
WMD	weapon/weapons of mass destruction

Bibliography

When a field manual has been published under a new number, the old number follows in parentheses.

DOCUMENTS NEEDED

These documents must be available to the intended uses of this publication. Most joint publications are available online: http://www.dtic.mil/doctrine/doctrine.htm. Most Army doctrinal publications are available online: http:// 155.217. 58.58.

JP 3-13. *Joint Doctrine for Information Operations*. 9 October 1998.

JP 3-51. *Joint Doctrine for Electronic Warfare*. 7 April 2000.

JP 3-53. *Doctrine for Joint Psychological Operations*. 10 July 1996.

JP 3-54. *Joint Doctrine for Operations Security*. 24 January 1997.

JP 3-57. *Joint Doctrine for Civil-Military Operations*. 8 February 2001.

JP 3-58. *Joint Doctrine for Military Deception*. 31 May 1996.

FM 3-0. *Operations*. 14 June 2001.

FM 5-0 (101-5). *Army Planning and Orders Production*. TBP.

When published, FM 5-0 will supersede that portion of FM 101-5 not superseded by FM 6-0.

FM 6-0. *Mission Command: Command and Control of Army Forces*, 11 August 2003.

FM 6-0 supersedes chapters 1 through 4 and 6, and appendixes G, and I through L of FM 101-5.

FM 6-20-10. *Tactics, Techniques, and Procedures for the Targeting Process*. 8 May 1996.

FM 6-20-10 will be republished as FM 3-60.

READINGS RECOMMENDED

These sources contain relevant supplemental information.

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/doctrine.htm.

JP 1-02. *DOD Dictionary of Military and Associated Terms*. 5 June 2003, as amended.

JP 2-0. *Doctrine for Intelligence Support to Joint Operations*. 9 March 2000.

JP 3-0. *Doctrine for Joint Operations*. 10 September 2001.

JP 3-09. *Doctrine for Joint Fire Support*. 12 May 1998.

JP 3-61. *Doctrine for Public Affairs in Joint Operations.* 14 May 1997.

JP 5-0. *Doctrine for Planning Joint Operations*. 13 April 1995.

JP 5-00.2. *Joint Task Force (JTF) Planning Guidance and Procedures.* 13 January 1999.

JP 6-0. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*. 30 May 1995.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: http://155.217.58.58/atdl.htm. Army regulations are produced only in electronic media. Most are available online: http://www.usapa.army.mil/USAPA_PUB_search_ p.asp.

AR 190-13. *The Army Physical Security Program.* 30 September 1993.

AR 360-1. *The Army Public Affairs Program*. 15 September 2000.

AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

AR 380-19. *Information Systems Security*. 27 February 1998.

AR 381-11. *Production Requirements and Threat Intelligence Support to the U.S. Army.* 28 June 2000.

AR 530-1. *Operations Security (OPSEC).* 3 March 1995.

FM 1 (FM 100-1). *The Army*. 14 June 2001.

FM 3-05.30 (FM 33-1). *Psychological Operations.* 19 June 2000.

FM 3-19.30 (FM 19-30). *Physical Security*. 8 January 2001.

FM 3-21.31. *Stryker Brigade Combat Team.* 13 March 2003.

FM 3-50. *Smoke Operations.* 11 September 1996.

FM 3-50 will be republished as FM 3-11.50.

FM 3-61.1. *Public Affairs Tactics, Techniques, and Procedures*. 1 October 2000.

FM 3-90. *Tactics*. 4 July 2001.

FM 3-93 (100-7). *The Army in Theater Operations*. TBP.

FM 3-100.12. *Risk Management: Multiservice Tactics, Techniques, and Procedures for Risk Management.* 15 February 2001.

FM 3-100.12 will be republished as FM 5-19.1.

FM 4-0 (100-10). *Combat Service Support.* 29 August 2003.

FM 6-02.2*. Command, Control, Communications, and Computers (C4) Operations: Interim Brigade Combat Team.* TBP.

FM 6-02.71. *Network Management*. TBP.

FM 6-20. *Fire Support in the AirLand Battle.* 17 May 1988.

FM 6-20 will be republished as FM 3-09.

FM 6-20-40. *Tactics, Techniques , and Procedures for Fire Support For Brigade Operations (Heavy)*. 5 January 1990.

FM 6-20-40 will be republished as FM 3-09.4.

FM 7-15. *The Army Universal Task List*. 31 August 2003.

FM 12-6. *Personnel Doctrine*. 09 September 1994

FM 12-6 will be republished as FM 1-0.

FM 20-3. *Camouflage, Concealment, and Decoys*. 30 August 1999.

FM 20-3 will be republished as FM 3-58.1.

FM 22-100. *Military Leadership*, 31 August 1999.

FM 22-100 will be republished as FM 6-22.

FM 27-100. *Legal Support to Operations*. 1 March. 2000.

FM 27-100 will be republished as FM 1-04.0.

FM 33-1-1. *Psychological Operations, Techniques, and Procedures*. 5 May 1994.

FM 33-1-1 will be republished as FM 3-53.10.

FM 34-1. *Intelligence and Electronic Warfare Operations*. 24 September.1994.

FM 34-1 will be republished as FM 2-0.

FM 34-2. *Collection Management and Synchronization Planning*. 8 March 1994.

FM 34-2 will be republished as FM 2-33.3.

FM 34-60. *Counterintelligence*. 3 October 1995.

FM 34-60 will be republished as FM 2-01.2.

FM 34-130. *Intelligence Preparation of the Battlefield*. 8 July 1994.

FM 34-130 will be republished as FM 2-01.3.

FM 41-10. *Civil Affairs Operations*. 14 February 2000.

FM 41-10 will be republished as FM 3-05.40.

FM 46-1. *Public Affairs Operations*. 30 May 1997.

FM 46-1 will be republished as FM 3-61.

FM 71-100. *Division Operations*. 28 August 1996.

FM 71-100 will be republished as FM 3-91.

FM 100-7. *Decisive Force: The Army in Theater Operations*. 31 May 1995.

FM 100-7 will be republished as FM 3-93.

FM 100-14. *Risk Management*. 23 April 1998.

FM 100-14 will be published as FM 5-19.

FM 100-15. *Corps Operations*. 29 October 1996.

FM 100-15 will be republished as FM 3-92.

FM 100-18. *Space Support to Army Operations*. 20 July 1995.

FM 100-18 will be republished as FM 3-14.

FM 100-25. *Doctrine for Army Special Operations Forces*. 1 August 1999.

FM 100-25 will be republished as FM 3-05.

FM 101-5-1. *Operational Terms and Graphics*. 30 September 1997.

FM 101-5-1 will be republished as FM 1-02.

DEPARTMENT OF DEFENSE PUBLICATIONS

DOD Directives are available online: http://www.dtic.mil/whs/directives.

DOD Directive S-3600.1. *Information Operations*. 9 December 1996.

DOD Directive 5100.77. *DOD Law of War Program*. 9 December 1998.

(FOUO) DOD Directive O-8530.1. *Computer Network Defense (CND)*. 8 January 2001.

PUBLIC LAWS AND OTHER PUBLICATIONS

Armed Forces Staff College Pub 1. *The Joint Staff Officer's Guide*. 1997.

Carter, Rosemary M. "The Information Operations Cell–Necessary for Division Offensive Actions." School of Advanced Military Studies monograph, Command and General Staff College, first term, AY 98-99.

Center for Army Lessons Learned (CALL) Newsletter 99-2. *Task Force Eagle IO: IO in a Peace Enforcement Environment*. January 1999.

Source for "CMO in a Peacekeeping Environment," page 2-25.

Center for Army Lessons Learned (CALL) Newsletter 99-15. *Tactics, Techniques and Procedures for Information Operations*. March 1999.

Source for "Maintaining the Initiative at Home Station," page 2-23.

CJCSI 3211.01C. "Joint Military Deception." 19 February 2002.

CJCSI 6510.01C. "Information Assurance and Computer Network Defense." 1 May 2001.

Concept for Future Joint Operations. *Expanding Joint Vision 2010*. May 1997.

General Order Number 5, Subject: Establishment of US Army Network Enterprise Technology Command/9th Army Signal Command; Transfer and Redesignation of The Headquarters and Headquarters Company, 9th Army Signal Command; Discontinuance of the Communications Electronic Services Office and the Information Management Support Agency. 13 August 2002.

Grohoski, Romanych, and Seybert, "Measures of Effectiveness in the Information Environment." *Military Intelligence Professional Bulletin* (July-September 2003): 12–16.

Paragraphs 6-16–6-38 and figures 6-1 and 6-2 use data from this article.

Information Assurance: Legal, Regulatory, Policy, and Organizational Considerations, 4th Edition. Washington, D.C.: The Joint Staff, Directorate of Command, Control, Communications, and Computer Systems. 25 August 1999.

Also called the "IA Purple Book".

Joint Pamphlet. *Information Assurance through Defense in Depth*. February 2000.

Joint Pamphlet. *Information Assurance. Legal, Regulatory, Policy and Organizational Considerations*, 4th Edition. August 1999.

Joint Pamphlet. *A Strategy for Peace the Decisive Edge in War, Information Operations*. March 1999.

Kahan, James P., D. Robert Worley, and Cathleen Stasz. "Understanding Commanders' Information Needs." RAND: Arroyo Center. June 1989.

LIWA. *Information Operations Planning, Tactics, Techniques, and Procedures for Field Support Teams, The Information Operations Process*, 6th Edition. May 1999.

Memorandum of Understanding Among Deputy Chief of Staff for Operations and Plans; Deputy Chief of Staff for Intelligence; Director of Information Systems for Command, Control, Communications, and Computers; and Commander, US Army Intelligence and Security Command, Subject: The US Army Intelligence and Security Command's Land Information Warfare Activity. February-March 1995.

Memorandum, DAMO-ODI, Subject*: Naming of the Armies Initial TOE, Information Operations Unit*. 14 August 2002.

Message: R51700Z OCT 00. From DA WASHINGTON DC//DAMO-ZA//, SUBJECT: Assignment of Army Component for Space/Computer Network Attack/Computer Network Defense.

Message: R011530Z NOV 00. FROM DA WASHINGTON DC//SAIS-IAS//,SUBJECT: New Information Assurance (IA) Personnel Status-Interim Policy Change.

Message: O12050Z NOV 00. FROM SECDEF, WASHINGTON DC//OASD-PA/DPL//. SUBJECT: *Public Affairs Guidance-Computer Network Attack*.

Message DTG 012050Z Nov 00, From SECDEF Washington DC//OASD-PA/DPL//, SUBJECT: *Public Affairs Guidance- Computer Network Attack*.

National Military Strategy. December 1999.

National Security Strategy for a New Century. December 1999.

Presidential Decision Directive 68. "United States International Information Policy (IPI)." 30 April 1999.

Smith-Mundt Act of 1948 (Title 22 USC section 1461).

The United States Code is available online: http://uscode.house.gov/usc.htm.

"Strategic Assessment, 1999." Institute for National Strategic Studies, National Defense University. June 1999.

Tulak, Arthur N. "The Application of Information Operations Doctrine in Support of Peace Operations." Master of Military Art and Science thesis, Command and General Staff College, 4 June 1999.

USAJFKSWCS Pub 525-5-15. *Psychological Operations: Capabilities and Employment*. January 1999.

US Army War College. "Strategic Research Project, Information Operations: A Layman's Perspective." 1 April 1997.

Index

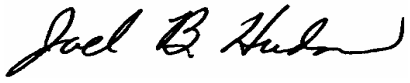
Entries are by paragraph number unless stated otherwise.

FM 3-13(FM-100-6)
28 NOVEMBER 2003

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:



JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
0331001

DISTRIBUTION:

Active Army, Army National Guard, and US Army Reserve: To be distributed in accordance with the initial distribution number 115425, requirements for FM 3-13.

PIN: 081127-000