MCWP 3-40.4

Marine Air-Ground Task Force Information Operations

U.S. Marine Corps

PCN 143 000140 00

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to **morgann@mccdc.usmc.mil**. Recommendations should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Add, delete
  - Proposed new text, preferably double-spaced and typewritten
- Justification and/or source of change

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status.* An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: **http://www.doctrine.usmc.mil**.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

9 July 2003

FOREWORD

Marine Corps Warfighting Publication (MCWP) 3-40.4, *Marine Air-Ground Task Force Information Operations*, operationalizes the concept of information operations (IO). This publication introduces doctrine for employment of IO in support of Marine air-ground task force (MAGTF) operations.

IO language and organizations continue to evolve and to be debated. This publication gives Marines a warfighter's orientation to IO, providing a basis to understand the relevance of IO and a framework to implement IO.

This publication is intended for MAGTF planners responsible for both operational and IO planning.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

EDWARD HANLON, JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

Publication Control Number: 14300014000

MAGTF INFORMATION OPERATIONS

TABLE OF CONTENTS

Chapter 3 Information Operations Capabilities

Chapter 4 Intelligence, Communications and Information Systems, and Information Management

Appendices

CHAPTER 1
FOUNDATION

"*War is both timeless and ever changing*."

MCDP 1, Warfighting

A Changing World

Marines play a vital role in the defense of the nation's interests. Marines support the nation's strategy through expeditionary operations, including peacetime engagement activities and combat. As the nation's expeditionary force in readiness, Marines will confront many new changes in the future. In the face of these new challenges, Marines must use all of their capabilities to the best possible advantage. These capabilities include the control and the use of information.

The world is going through dynamic changes that will alter the operational environment in which Marine Corps forces will deploy and fight. These changes have been brought about by many factors. The rapid advance of technology and the resultant proliferation of increasingly powerful asymmetric weapons, the emergence of diverse adversaries, and the Marine Corps' involvement in humanitarian and peace operations contribute to a new and increasingly complex operational environment.

Technology Advance

The rapid advance of technology has been a powerful force for change. It has brought new capabilities as well as new challenges. Communication systems have been enhanced through networking. Advances in computing power have allowed improved processing and display of intelligence and battlefield information. In many ways, information has emerged as a critical aspect of command and control (C2), strategic agility, and operational maneuver.

However, these advantages are accompanied by new dangers. These dangers exist as new and critical vulnerabilities. New systems may be vulnerable to disruption by computer viruses, hackers, and simple misuse. Many new global and garrison communication systems share the same infrastructure as public communications. Many countries and adversaries have access to similar technologies on the global market. The difference between military and civilian technology is decreasing.

Future Adversaries

The global strategic environment remains complex and potentially dangerous. Marines still face a range of traditional and non-traditional threats. Ethnic, economic, social, and environmental strains will continue to cause instability and raise the potential for violence. Many countries will retain the capability to threaten United States (US) interests abroad, and may seek to initiate a major conflict that would require a large-scale US response. In addition, there will be many other "lesser threats" that will seek to engage us across the range of operations that fall short of war. These adversaries will generally possess a regional or national level of influence, and will likely have access to lethal technologies generally available on the global market.

Some examples include terrorists, drug cartels, computer hackers, and rogue nations—who might act independently in their own self-interest. Using new technologies and readily available information, these threats will have the capability to

threaten the US across geographic borders through networks and through the proliferation of weapons of mass destruction. They may avoid direct military confrontation and attack selected vulnerabilities to achieve a high payoff for little cost or they may attack to simply gain media exposure.

Future Missions

The US maintains a wide range of humanitarian and global security responsibilities, and these responsibilities will continue well into the future. Marines can expect to be tasked for the following:

- Provide humanitarian assistance (domestic or foreign) after a disaster.
- Provide peace support for nations that seek a secure environment to peacefully develop.
- Provide peace enforcement to separate warring factions.
- Create conditions for the peaceful resolution of a crisis.
- Project combat power when resolving a crisis that requires the threat and/or use of force.

As a crisis develops, Marines may find themselves executing multiple missions simultaneously or in rapid sequence. They may be asked to provide relief to civilians while keeping belligerents separated, defending US interests, and enforcing international law. To project power and influence, Marine Corps forces employ for presence, engagement, and response. Each will have a strong informational component. The on-scene presence of the forward-deployed Marine Air-Ground Task Force (MAGTF)—and its proximity and access to potential crisis areas—will establish it as a vital operational and informational cornerstone for follow-on forces acting as part of a national and theater crisis response.

Expeditionary Operations

An expedition is a military operation conducted by an armed force to accomplish a specific objective in a foreign country. The missions of military expeditions vary widely and expeditionary operations occur across the continuum of peace, crisis, and war. Examples of missions of military expeditions include the following:

- Provide humanitarian assistance (domestic or foreign) in times of disaster or civil disruption.
- Establish and keep the peace in a foreign country.
- Protect US citizens or commerce abroad.
- Retaliate for an act of aggression by a foreign political group.
- Thwart transnational terrorist and criminal threats.
- Protect US interests by defeating enemy armed forces in combat.

The fundamental nature of war—a violent struggle between two hostile, independent wills—will remain unchanged. The quantitative characteristics of warfare (mass and volume) are essential elements of combat power. However, qualitative factors (speed, stealth, precision, and sustainability) are increasingly important. Maneuver and decisive action lead to the accomplishment of the mission. In disasters, they include relief operations. In civil disruptions, they often include peace operations until local government control can be re-established. In conflict, they involve the military defeat of the enemy's fighting forces.

Marine Corps information operations (IO) support maneuver warfare through actions that use information to deny, degrade, disrupt, destroy or influence an adversary commander's methods, means or ability to C2 his forces and to inform

target audiences through informational activities. IO enhance the ability of the MAGTF to project power during peace and war. They complement and facilitate the traditional use of military force but in some instances may stand alone as a deterrent option. IO support the integration of situational awareness, operational tempo, influence, and power projection to achieve advantage.

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

IO is multi-disciplined. Capabilities relevant to IO include, but are not limited to, psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), physical attack, information assurance (IA), computer network operations (CNO), public affairs (PA), and civil-military operations (CMO). IO conducted by MAGTFs support battlespace shaping, force enhancement, and force protection activities. IO will enhance the ability of the MAGTF to project power during peace and war, complementing and facilitating the traditional use of military force.

MAGTFs will execute IO to enable and enhance their ability to conduct military operations consistent with the Marine Corps' capstone concept, *Expeditionary Maneuver Warfare (EMW)*. The MAGTF can support joint and multinational enabling by serving as an adaptive cornerstone force-bringing flexible command, control, communications, computers, and intelligence (C4I) systems that allow a joint or coalition force to be assembled in an expeditionary environment. Marines also bring unique capabilities such as the electronic attack (EA)-6B Prowler and the Mobile Electronic Warfare Support System-adding to the combat power of the joint force. IO can increase strategic agility by utilizing the reach back capability of MAGTF command, control, communications, and computers (C4) systems thus allowing the MAGTF to draw upon information sources outside its area of operations. IO can extend operational reach through informational and media activities that unify power projection with influence projection. IO can increase tactical flexibility by providing the MAGTF commander with a range of both lethal and nonlethal options. Finally, IO can enhance support and sustainment by enabling power projection against distant targets without increasing the MAGTF's footprint ashore.

Principles

The following principles are essential to the successful integration of IO within the MAGTF:

- *IO is an integral function of the MAGTF.* Marines organize as unique, task-organized MAGTFs. The ability to integrate combat power to win in conflict is inherent in Marine Corps organization and the expeditionary mindset of the individual Marine. Marines intuitively understand task organization. Integration of capabilities is a part of how Marines fight. MAGTF IO planning is inherent to MAGTF planning and is not conducted by unique IO forces.
- *MAGTF IO is focused on the objective.* Like all operations, information operations ultimately exist to help the MAGTF achieve its mission. A thoughtful analysis of the MAGTF mission and a subsequent strategy-to-task analysis of IO activities are essential. No activity exists independent of the compelling requirement for the MAGTF to meets its objective. A carefully structured IO plan preserves MAGTF resources and assists the MAGTF in synchronizing the activities of external agencies with those of the MAGTF.
- *The MAGTF commander's intent and concept of operations determine IO targets and objectives.* The MAGTF should determine the vulnerabilities and critical elements of friendly and enemy information, information-based

processes, and information systems. Key adversary elements, the destruction or degradation of which would support the accomplishment of the unit mission, should be targeted as a system. Likewise, the MAGTF's adversaries will target MAGTF C2 systems; therefore, friendly systems critical to the MAGTF should be protected. Integration and coordination of influences such as media, messages, and personal contact should be exercised to the advantage of the MAGTF. In all cases, whether attacking the adversary, defending the MAGTF's own systems or managing influences, the targets and objectives are determined by the MAGTF commander's intent and the concept of operations.

- *MAGTF IO must be synchronized and integrated with those of the higher and adjacent commands.* IO will be conducted in battlespace that has already been shaped by the combatant commanders' peacetime theater security and cooperation activities. During joint operations, the joint force commander (JFC) provides guidance and direction for conducting IO to support his mission, concept of operations, objectives, and intent. The MAGTF IO plan, while leveraging and exploiting the IO capabilities of higher echelons in support of MAGTF objectives, must also support the JFC's IO objectives.
- *MAGTF IO is supported by the total force.* Not all IO activities that support the MAGTF are conducted by the MAGTF. For example, computer network monitoring is conducted by the Marine information technology network operations center and intelligence support is contributed by the Marine Corps intelligence activity. Marine Corps reserve component assets are available to provide civil affairs (CA), and other expertise.
- *Many different capabilities and activities must be integrated to achieve a coherent IO strategy.* The support of the warfighting functions of the MAGTF (maneuver, fires, logistics, force protection, intelligence, and C2), as well as the design and operation of information systems, are critical to the successful conduct of IO.
- *Intelligence support is critical to the planning, execution, and assessment of IO.* IO requires accurate, timely, and detailed intelligence, to include intelligence preparation of the battlespace (IPB) products. An early assessment of key enemy centers of gravity (COGs) is essential. Intelligence analysis should determine the enemy's potential IO vulnerabilities and capabilities, and support friendly IO actions to exploit or to counter them. Analysis may also help in defining suitable measures of effectiveness for specific IO actions.

Information and the Range of Military Operations

IO include all actions taken to affect enemy information and information systems while defending friendly information and information systems. Information, as data, is a key component of combat, communications, and intelligence systems. Information transformed into knowledge and understanding is a key component of command and decisionmaking processes. Information, as media, influences perceptions, attitudes, and beliefs. Information and information systems are targets that, when affected, influence key decisionmakers.

IO is conducted during all phases of an operation, across the range of military operations, and at every level of war. In some environments IO capitalizes on the growing sophistication, connectivity, and reliance on information technology. IO focuses on the vulnerabilities and opportunities presented by the increasing dependence on information and information systems.

In other situations, IO may mean employing decidedly low-tech means, such as exploiting

cultural factors or a less sophisticated means of communication, to facilitate CMO, to influence selected target audiences or by tactical deception. Whatever the nature of the conflict, IO target information or information systems to affect the information-based decisionmaking process. IO may, in fact, have its greatest impact as a deterrent in peace and during the initial stages of crisis. IO may help deter adversaries from initiating actions detrimental to the US. At every echelon of command and all levels of warfare, the use of information is likely to be a critical tool in achieving the objectives of the commander. IO will primarily support battlespace shaping, force enhancement, and force protection actions, and any other information-oriented activity the MAGTF can leverage to better facilitate the tailored application of combat power.

Battlespace Shaping

The US seeks to shape the international environment through a variety of means, including diplomacy, economic cooperation, international assistance, security assistance, and arms control. These efforts use power, information, and influence to achieve national objectives. In peacetime, deployed Marine Expeditionary Units (MEUs) demonstrate national resolve through forward presence, and Marines enhance regional stability through cooperative engagement, with allies in exercise, exchange, and informational programs. During crises, MAGTF-shaping operations must be linked to US strategic objectives and be consistent with on-going regional engagement activities. During conflict, MAGTF-shaping operations focus on setting those conditions necessary for operational and tactical success.

Whether demonstrating national commitment through forward presence, exercising with allies and strategic partners, engaging in armed combat or providing relief to victims of a natural catastrophe, Marines will continue to support the nation's objectives and policies. IO, used in support of battlespace shaping, ensures the purpose of the MAGTF's mission is clear to both the local and the worldwide audience.

Strategic Focus

MAGTF operations efforts will be observed, commented upon, and selectively portrayed to, and by, the world audience. Actions will be perceived differently by viewers who may likely be biased. The perceptions created by MAGTF operations will result in changes to political realities that may, in turn, affect the assigned MAGTF mission. Information is a powerful component of battlespace shaping. Not only do actions matter, but the perceptions that actions create matter. Small, apparently local actions may have strategic consequences. For example, an "event" at a single checkpoint can change the relationship between the MAGTF, local residents, allied partners, and nongovernmental organizations (NGOs) and-depending upon how the event is portrayed through the media-can dramatically sway public opinion either for or against actions. In the battlespace of the future, all Marines must be aware of their strategic responsibilities.

Multinational Partners

MAGTF operations will likely involve coordinated activities with the armed forces of other nations in a multinational effort, and future allies will all have different capabilities, equipment, procedures, and values. MAGTF operations must carefully consider the implications of actions taken by members of the multinational force. The human dimension of coalition operations must be considered, and used to effectively form and employ the force.

Civil Considerations

All military operations, from major theater wars to the complex contingencies encountered in other expeditionary operations, will occur in an

inherently uncertain and chaotic environment shaped by continuous human interaction. Civilian populations, organizations, and leaders will cause much of this uncertainty, and the commander must shape the battlespace within this context of unpredictability. Battlespace shaping helps commanders simultaneously meet their own operational requirements and their moral and legal responsibilities to civilians.

Integrated Targeting

The integrated use of informational activities and fires, both lethal and nonlethal, to achieve a common purpose is essential. The targeting means is secondary to achieving the desired targeting effect since targets no longer reside solely in the physical domain but include the perceptions and actions of civilians, key leaders, and adversaries. Information can be used for a positive purpose to achieve desired operational effects while mitigating the unnecessary loss of life.

During conflict, the MAGTF will necessarily focus on the battlespace's physical and informational aspects that affect decisive maneuver. However, the use of IO to shape the battlespace transcends the physical domain. It must also consider the political, cultural, and moral aspects of the battlespace. As crisis blends into conflict, the defining point when operations change from peace support, to peace enforcement or to conflict will become increasingly difficult to define. It will require Marines to approach operations holistically, with an understanding of the historical underpinnings and cultural aspects of the crisis or conflict, an understanding of the ability of information and influence to achieve desired operational effects, and an understanding of their responsibilities to terminate conflict in a manner that will foster lasting stability.

Force Enhancement

Networking and advances in computing power have allowed improved processing and display of intelligence and battlefield information. In many ways, the ability to obtain timely and accurate information has emerged as a critical aspect of C2, strategic agility, and operational maneuver. The force that best controls, utilizes, and safeguards information and information systems has always enjoyed a decided military advantage; this will not change.

As a force enhancer, IO integrate varied capabilities and activities into a coherent, seamless plan to achieve specific objectives. The human decisionmaking process is the ultimate target. Guidance must be clearly established, support overall national and military objectives, consider the influence of other regional informational activities taking place outside the MAGTF, and include identifiable measures of effectiveness. A close and continuous relationship between IO and intelligence support is essential.

Operational Focus

The primary focus of MAGTF offensive IO activities will be at the operational and tactical levels of war. Actions will be oriented against C2 targets to disrupt, degrade or deny an enemy's use of information and information systems to achieve operational objectives. A principal focus of IO at this level is the enemy commander and his decisionmaking process. By targeting the human element, the MAGTF seeks to affect the adversary's will to resist and destroy his military operational effectiveness. Integrated targeting to achieve the desired operational effects will combine influence, information, and weapon effects to shape the physical, electronic, and informational aspects of the battlespace.

The mission and the MAGTF commander's intent are paramount. All MAGTF IO elements must work together to produce a synergistic effect. During conflict, the MAGTF may rely heavily upon EW, military deception, and physical destruction to attack C2, intelligence, and other critical information-based processes that directly impact an adversary's ability to conduct

military operations. The MAGTF may rely on national-level agencies and other Service components for certain offensive IO-related capabilities not inherent to the MAGTF.

Integration

Offensive IO involves the integrated use of supported and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decisionmakers and their information and information systems. These capabilities and activities include, but are not limited to OPSEC, military deception, PSYOP, EW, physical attack, and CNO. The human decisionmaking process is the ultimate target for offensive IO.

Nodal Analysis

The analysis of the adversary's C2 system to determine critical and vulnerable nodes is called nodal analysis. During planning, it is essential that IO planners consider the adversary's C2 network as a system that is made up of personnel, equipment, information, and procedures that work together to allow the adversary commander to accomplish the mission. Also included in the adversary's C2 system are adversary perceptions, decisions, and reactions. Thus, offensive IO target adversary C2 systems; for example, radars, communication nodes or information systems, as well as the decisionmaker and his decision cycle including the mind of the enemy commander, command nodes or intelligence systems. Offensive IO support the mission and the commander's intent. These operations are based on a clear understanding of the friendly mission and a thorough analysis of the enemy C2 system (including biases and decisionmaking processes).

Objectives

Offensive IO objectives must be clearly established. They must support overall national and military objectives and include identifiable indicators of success. Selection and employment of specific offensive capabilities against an enemy must be appropriate to the situation. Offensive IO may be the main effort, a supporting effort or a phase in the MAGTF operation. Offensive IO objectives include the following:

- Influence the adversary commander's estimate of the situation.
- Slow the adversary's tempo of operations.
- Degrade the adversary commander's decision cycle for planning and executing operations.
- Disrupt the adversary commander's ability to generate and focus combat power.

Employed as an integrating strategy, force enhancement activities weave together related offensive IO capabilities and informational activities toward satisfying a stated objective. Offensive IO degrade the flow of information through EW and physical attack/destruction and influence enemy information through PSYOP, OPSEC, and military deception. The integrated use of these methods disrupts the enemy decisionmaking process.

Force Protection

The MAGTF commander depends on information to plan operations and employ his forces. Information systems enable and enhance warfighting capabilities; however, increasing dependence upon these rapidly evolving technologies may create new vulnerabilities. Seabasing of the MAGTF simultaneously makes IA more robust and more difficult to provide. Risk management decisions will have to be made based on the anticipated requirements and information resources most needing protection. The integration of protection, detection, and reaction capabilities is needed to mitigate the effects of enemy action and environmental effects. It enables the necessary protection

of information and information systems on which the MAGTF depends to conduct operations and achieve its objectives. The criticality of the MAGTF commander's access and use of the information environment will not go unnoticed by future adversaries. IO will enhance force protection by protecting and defending the information and information systems that the MAGTF depends on to conduct operations.

Integration

Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Offensive action can be used to pre-empt or to respond to adversary IO capabilities. Defensive IO are conducted and assisted through information assurance, OPSEC, physical security, counterdeception, counterpropaganda, counterintelligence (CI), and EW. During operational planning, an analysis of friendly information systems and their vulnerabilities, such as nodal analysis, is conducted with a risk assessment to determine defensive IO measures and priorities.

Defense in Depth

Defensive IO ensure timely, accurate, and relevant information access while denying the enemy the opportunity to exploit friendly information and information systems for its own purposes. Since it is a practical impossibility to defend every aspect of the infrastructure and every information process, defensive IO provide the essential and necessary protection and defense of information and information systems upon which the MAGTF depends to conduct operations and achieve objectives. A useful guide is Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01C, Information Assurance and Computer Network Defense. Security requirements and procedures for defense-in-depth strategy may be found in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, Information Assurance Implementation Procedures. This manual includes such areas as individual responsibilities, system administrator training requirements, Information Assurance Vulnerability Alert (IAVA), incident reporting, information operations conditions (INFOCONs), communications security (COMSEC), and specific defense-in-depth minimum-security requirements that may be useful in developing defensive IO plans.

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

Objectives

The objectives of defensive IO include the following:

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

Defensive IO plans ensure effective friendly use of the electromagnetic spectrum while negating adversary efforts to do the same. Defensive IO reduce friendly C2 vulnerabilities to adversary attack by employing adequate physical, communications, electronic, and OPSEC measures. Ongoing coordination and deconfliction are required to reduce friendly mutual interference and manage the electromagnetic spectrum in support of friendly C2.

CHAPTER 2
INTEGRATION AND PLANNING

"During times of peace, the most important task of any military is to prepare for war."

MCDP 1, *Warfighting*

The Marine Corps Component

The Marine Corps component is responsible for setting the conditions and creating the environment for successful joint MAGTF operations. The Marine Corps component commander advises the JFC of the IO capabilities of his forces, makes recommendations on the proper employment of Marine Corps forces, requests additional IO support as required, and informs the JFC regarding the Marine Corps component's IO situation and progress.

With respect to IO, the Marine Corps component commander focuses on those activities that will support future operations—the next Marine Corps component mission—and coordinates IO actions with other component commanders to achieve unity of effort for the joint force. The IO orientation of the Marine Corps component commander is normally at the operational level of war, while the MAGTF commander is normally at the tactical level. Naturally, there will be some overlap. The Marine Corps component provides the following IO support:

- Plans access to national, theater, and joint task force (JTF) intelligence system architectures and databases in conjunction with the component intelligence staff.
- Develops component IO policy as needed consistent with the JFC's IO policies.
- Ensures that the capabilities of the Marine Corps are integrated in the operation plans (OPLANs), contingency plans, and future plans of the combatant commander.
- Represents Marine Corps forces in the joint force IO cell and at joint boards as required; e.g., targeting and intelligence to set conditions favorable to the MAGTF's mission accomplishment.

For more information regarding component responsibilities, see MCDP 1-0.1, *Componency* (to be reissued as MCWP 3-40.8).

The Total Force

The Marine Corps organizes, equips, trains, and fights as a total force. Effective IO integration requires that the total capability of the Marine Corps be used to support the warfighting MAGTF.

The Marine Corps Reserve augments and reinforces the active duty forces in time of war or national emergency. They support the rapid expansion of the Marine Corps and provide added capability, flexibility, and depth to the active duty force. Marine Corps CA units consist of two civil affairs groups (CAGs). The CAGs are selected Marine Corps Reserve units. Understanding the civil dimension of crisis and conflict is important to IO. The CAGs provide a unique capability to the MAGTF to address civil considerations.

Operational Focus

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

Offensive IO actions will be oriented against C2 targets, disrupting or denying an enemy's use of information and information systems to achieve operational objectives. The MAGTF may rely most heavily on EW, deception, and/or physical destruction to attack targets related to C2, intelligence, and other critical information-based processes directly related to conduct military operations. Defensive IO actions will protect and defend the information and information systems that the MAGTF depends on to conduct operations. The MAGTF will frequently rely on national-level agencies and other Service components for certain offensive and defensive IO-related capabilities. Informational activities will be needed to manage media attention on the operation, influence selected adversary groups, and protect MAGTF information and information systems.

Since MAGTFs may fight as a part of a larger joint force, their offensive, defensive, and informational IO efforts will support and be coordinated with the campaign plans of the combatant commander, joint force, and adjacent commands. The JFC may have standing IO procedures and perhaps a standing IO plan based on the combatant commander's guidance for the theater of operations and the nature of the conflict. The joint force and component commanders in turn will develop their own IO plans in support of their respective objectives. These IO plans will be largely at the operational level. The MAGTF will develop an IO plan that will support MAGTF mission requirements while integrating into the JFC IO plan. In turn, the major subordinate commands will need to develop supporting IO plans appropriate for their level of command.

Staff Responsibilities

Operations

The G-3/S-3 is responsible for IO. The future operations section is responsible for overseeing the planning and coordination of the IO effort.

The MAGTF IO officer, within G-3/S-3 future operations, is responsible for:

- The broad integration and synchronization of IO efforts.
- Responding directly to the G-3/S-3 for MAGTF IO.
- Ensuring that the IO cell provides input to the operational planning team (OPT) during planning to ensure coordinated operations.
- Preparing the IO appendix to the operation order (OPORD).
- Overseeing the core personnel within the IO cell as well as augmentees from external agencies.
- Ensuring that all IO matters are coordinated within the MAGTF staff, higher headquarters, and external agencies.

The electronic warfare officer (EWO) integrates EW operations through the EW coordination center or the IO cell when established.

The fire support coordinator, supporting arms coordinator, target information officer, and target intelligence officer oversee the formation of the target list and the engagement of those targets.

Intelligence

Intelligence support is critical in the planning, execution, and assessment of IO and must provide support across the full range of military operations, at all levels of war.

The G-2/S-2 acts as the central point of contact for all intelligence support to IO for the MAGTF staff. Coordination and interaction between the G-2/S-2 and the G-3/S-3 may be enhanced through liaison representatives embedded within the IO cell. See also appendix A, Information Operations Cell Responsibilities.

Communications and Information Systems

The G-6/S-6 assists in prioritization of the defensive information operations effort, oversees the COMSEC program, supports the installation and

maintenance of information systems, and assists the EWO in deconflicting EW jamming operations.

The Information Operations Cell

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

During planning, the IO cell should facilitate coordination between various staffs, organizations, and the MAGTF staff elements responsible for planning specific elements of IO. During execution, the cell should remain available to assist in coordination, provide support or adjust IO efforts as necessary. The IO cell should have the communications connectivity, either through the combat operations center or separately, to effectively coordinate changing IO requirements.

The IO cell is composed of intelligence personnel, augmentees supporting IO activities, and representatives from staff elements and subject matter experts from appropriate warfighting functions. The size and structure of the cell are tailored to meet the mission and the commander's intent. Cells that are too large and over-manned can be as detrimental to the success of IO as those that are under-manned.

Operationalizing Information Operations

IO is a combination of battlespace shaping, force enhancement, and force protection activities that are integrated and concurrently planned. Essentially, force protection is a defensive shield to protect our own systems and decision processes, while force enhancement is the offensive sword used against the adversary. However, IO goes beyond attack and defense. It includes those actions taken to influence selected groups and decisionmakers and establishes battlespace conditions conducive to success. Therefore, it is necessary to include the concept of battlespace shaping. See figure 2-1 on page 2-4.

Battlespace shaping combines PA, OPSEC, concealment and deception, PSYOP, and the threat and/or use of force. It encompasses all actions taken to convey (or deny) selected information and images to an audience in order to influence and inform. Battlespace shaping occurs within both the informational and the physical domains. It requires the broad synchronization of PSYOP, PA, OPSEC, deception, and operations within a single battle concept.

MAGTF planners must ensure that IO planning begins at the earliest stage of operational planning, is consistent with the IO plans of the higher headquarters, and is fully integrated into the concept of operations.

Marines use the Marine Corps Planning Process (MCPP) to plan operations. The MCPP is a logical problem solving process used to develop a comprehensive and synchronized plan to accomplish the mission. One of the functions of the MCPP is to develop courses of action (COAs). IO planning naturally focuses on the IO COA within the overall planning process.

Integrated Information Operations Planning and the Marine Corps Planning Process

To understand how IO planning might be accomplished, it can be broken into steps. The following example is not intended to dictate planning procedures to MAGTFs. It is an illustration that allows Marine planners to begin to operationalize IO concepts. A disciplined IO planning process helps keep IO planning 'in step' with other

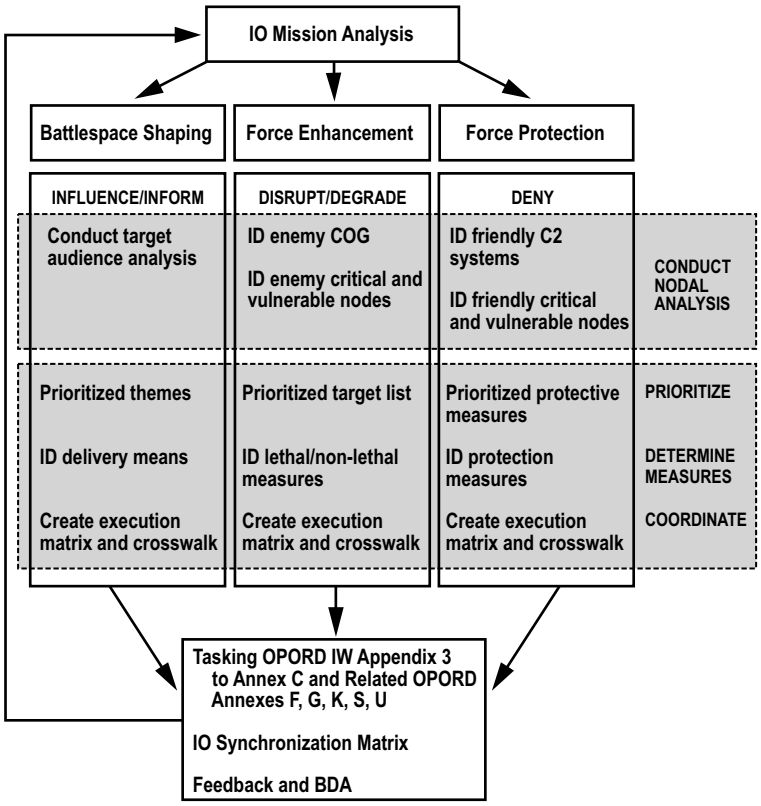

Figure 2-1. Information Operations Planning.

planning efforts. It allows targets, informational themes, and tasks to be logically derived.

Target and intelligence analysis is essential in IO planning. Integration and planning efficiency is achieved by conducting IO analyses simultaneously across functional areas. For example, nodal analysis is conducted simultaneously to determine key friendly nodes, key enemy nodes, and key target audiences. Then, each node (or COG) is subsequently prioritized (according to commander's guidance and desired effect), has specific IO measures (proposed tasks) placed against it, and is coordinated within the MAGTF operational scheme (by IO cell and OPT). IO tasks and guidance form the basis for the IO related sections of the OPORD. Finally, the establishment of feedback mechanisms and battle damage assessment (BDA) cycles permit the on-going evaluation of operations.

The MCPP supports decisionmaking by the commander. It is also a vehicle that conveys the commander's decisions to his subordinates and helps organize the thought processes of a commander and his staff throughout the planning and execution of military operations. The MCPP focuses on the mission and the threat. It capitalizes on the principle of unity of effort and supports the establishment and maintenance of tempo. The MCPP is applicable across the range of military operations and is designed for use at any echelon of command. The process can be as detailed or as abbreviated as the situation permits.

The MCPP organizes the planning process into six manageable, logical steps. See figure 2-2. It establishes procedures for analyzing a mission, developing and wargaming COAs against the threat, comparing friendly COAs against the

commander's criteria and each other, selecting a COA, and preparing an OPORD execution. It provides the commander and his staff a means to organize their planning activities and transmit the plan to subordinates and subordinate commands. IO planning is aligned with the MCPP steps and ensures IO actions are coordinated with all six warfighting functions and the operations of higher, adjacent, and subordinate commands.

IO planning is conducted within the framework of the MCCP. It is conducted in alignment with the tenets of top-down planning, the single-battle concept, and integrated planning. Top-down planning and the single-battle concept ensure unity of effort, while the warfighting functions (C2, maneuver, fires, intelligence, logistics, and force protection) serve as the building blocks of integrated planning.

Mission Analysis

Mission analysis is the first step in the MCPP. The purpose of mission analysis is to review and analyze orders, guidance, and other information provided by higher headquarters, and produce a unit mission statement. Mission analysis drives the MCPP.

The higher headquarters order is analyzed to extract IO planning guidance such as constraints, restraints, and planning factors. This guidance establishes the boundaries for IO planning, identifies target limitations based on policy and rules of engagement (ROE), and helps reduce the uncertainty associated with IO planning. This process also ensures that the MAGTF will nest its IO plan with that of the higher headquarters.

During mission analysis, IPB planning supports the commander as he develops his battlespace area evaluation. Assisted by the intelligence section, the MAGTF IO cell reviews known facts about the enemy C2 systems and the battlespace environment. IPB products relevant to further IO planning are developed or requested. Enemy COGs are determined. Potential risks and friendly vulnerabilities are also identified for defensive IO actions. Information gaps must be determined and requests submitted to resolve the uncertainties necessary for further planning. Unique IO factors, such as IO ROE and assumptions, are identified

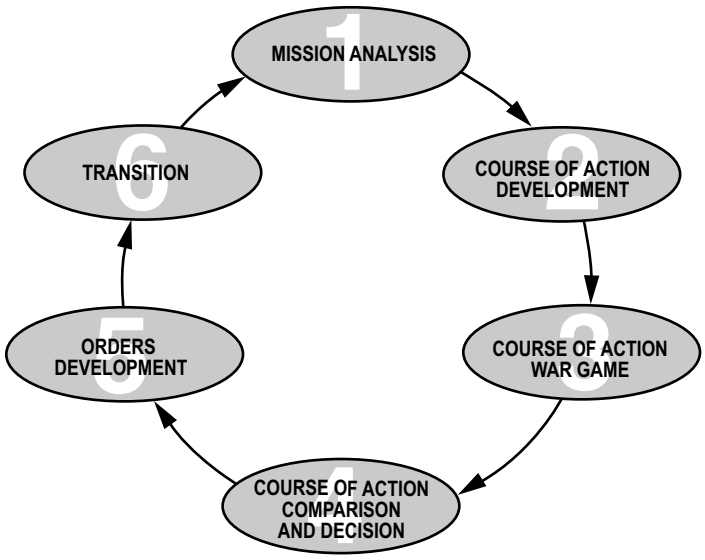

Figure 2-2. The Marine Corps Planning Process.

during mission analysis. IO planners conduct a strategy to task analysis that links the MAGTF mission to strategic and operational IO objectives.

An initial concept for IO support can be developed during mission analysis. Friendly IO assets and capabilities, either organic or supporting the MAGTF, as well as additional IO force structure requirements, are identified. As mission analysis is conducted, resource or capability shortfalls are noted. The IO cell should identify critical shortfalls and request support from higher headquarters or external agencies. Desired results should be determined. The IO concept of support must be focused by and in accordance with the commander's initial guidance. A staff estimate for IO is the most formal form of this concept of support and should be considered.

The IO cell must fully participate in MAGTF planning activities and coordinate its planning efforts with those of the MAGTF future operations section. Future operations will usually form an ad hoc organization known as the OPT. The OPT will be conducting mission analysis, and results of each group's (OPT and IO cell) analyses should be combined. Friendly vulnerabilities can be incorporated into force protection planning, while the enemy critical vulnerabilities determined through the OPT's COGs analysis could include potential IO targets. Emerging themes and messages that can influence the battlespace to the advantage of the MAGTF can become the basis for an overall perception management operation.

During mission analysis, IO planning results should be incorporated into the commander's planning guidance, IPB products, commander's critical information requirements (CCIRs), COG analysis, and staff estimates.

The most critical element to address during mission analysis is the integration of IO into the commander's vision of shaping actions. IO must be integral to the MAGTF shaping effort. Shaping sets conditions for decisive actions. They are activities conducted throughout the battlespace to influence an enemy capability, force or the enemy commander's decision. The commander shapes the battlespace principally by protecting friendly critical vulnerabilities and attacking enemy critical vulnerabilities.

Course of Action Development

During COA development, planners use the mission statement, commander's intent, and commander's planning guidance to develop the COAs. Each prospective COA is examined to ensure that it is suitable, feasible, acceptable, distinguishable, and complete with respect to the current and anticipated situation, mission, and commander's intent.

Planning started during mission analysis will continue in COA development. The IPB products requested and developed will be reviewed for applicability with the commander's planning guidance. As necessary, IPB products will be modified and updated. As new information is received, CCIRs may be revised and additional requirements submitted.

IO cell planning efforts will continue to be closely linked with those of the OPT. To assist the OPT, the IO cell may graphically display friendly and enemy IO assets as well as enemy C2 links and nodes to allow the planners to see the current and projected capabilities of both friendly and enemy forces. In coordination with the red cell and the G-2, the IO cell will conduct nodal analysis to assess relative IO capabilities and provide the OPT with an understanding of the strengths and weaknesses of both friendly and enemy forces. The IO cell will conduct an assessment of friendly vulnerabilities to enemy IO actions. The IO cell will also continue to refine its analysis of the enemy COG to determine the

critical enemy vulnerabilities most susceptible to IO. The refined COGs and critical vulnerabilities are used in the development of the initial COAs.

The IO cell will closely follow the development of the OPT COAs to ensure that the IO concept of support adequately supports these COAs. The IO cell may formulate an IO concept of support that will identify IO actions to be implemented regardless of the eventual COA that is adopted. In addition, the IO cell may create a concept of support for every COA developed by the OPT. Just as every COA will have to meet the OPT's criteria for suitability, feasibility, acceptability, distinguishability, and completeness, the IO cell must ensure that the IO concept of support can pass similar review. Each IO concept of support must address the following:

- What IO tasks will be accomplished?
- Who (IO assets) will execute the tasks?
- When will the IO tasks occur?
- Where will the IO tasks occur?
- Why is each IO task required?
- How will the MAGTF employ the IO capabilities to accomplish the tasks, and how is the IO concept nested with the higher headquarters' IO plan?

At the conclusion of COA development, the OPT or IO cell should have developed the following:

- An overall IO concept.
- An IO concept of support for each COA.
- Recommendations for the commander's wargaming guidance and evaluation criteria.
- Updated IO associated IPB products.
- Input to the COA graphic and narrative.
- An initial staff estimate for IO with additional asset requirements identified as appropriate.

Course of Action War Game

COA wargaming may involve a detailed assessment of each COA relative to the enemy and the battlespace. Each friendly COA is wargamed against selected threat COAs. COA wargaming assists the planners in identifying strengths and weaknesses, associated risks, and asset shortfalls for each friendly COA. COA wargaming will also identify branches and potential sequels that may require additional planning. Short of actually executing the COA, COA wargaming provides the most reliable basis for understanding and improving each COA.

The IO cell participates fully in the COA war game. Its objective in the war game is to refine and validate both the overall IO concept of support as well as the specific IO concepts of support for each COA. The IO actions are integrated into the COA war game in an interactive process to determine the impact on both friendly and enemy capabilities. The IO cell should observe and record the advantages and disadvantages of each COA and the capability of IO to support each. It should also identify possible branches and potential sequels in the IO concept for further planning.

At the conclusion of the COA war game, the IO cell reviews its planning products and refines them to support the next step in the MCPP. These planning products include the following:

- Updated IPB products.
- Refined staff estimate for IO.
- Refined CCIRs.
- Task organization and asset shortfalls for IO resources.
- IO input to COA synchronization matrix.

Course of Action Comparison and Decision

In COA comparison and decision, the commander evaluates all friendly COAs against his established criteria, then against each other, and then selects the COA that will best accomplish the mission.

As appropriate, the IO cell may provide additional comparison criteria directly relevant to IO that may assist the commander in his decision. The IO results from the COA war game may be briefed as

a separate, supporting concept by the IO cell or presented by the OPT as an element of the overall plan. In any event, the IO cell is responsible for ensuring that the impact and anticipated effect of IO actions upon the enemy for each COA, and the relative merit of each COA from an IO perspective are provided to the commander.

Orders Development

During orders development, the staff takes the commander's COA decision, mission statement, commander's intent, and guidance, and develops orders to direct the actions of the unit. Orders serve as the principal means by which the commander expresses his decision, commander's intent, and guidance.

The IO cell is responsible for taking the overall IO concept of support and the concept of support specific to the COA selected by the commander and turning them into appropriate sections of the OPORD under the direction of the MAGTF IO officer. Although the bulk of IO will be contained in Annex C, Operations, Appendix 3, IO can also be addressed in various other sections of the OPLAN. During orders reconciliation and crosswalk, the IO cell may be called upon to review the IO sections of the orders, identify gaps in planning or discrepancies, and provide corrective action. IPB products to support orders development are finalized. If fragmentary orders are issued, then the IO cell will ensure that appropriate instructions are given to IO capable units.

IO must effectively support combat operations. To achieve this, the IO plan must be developed early, it must be fully integrated into the overall operational plan, and it must be continually updated in view of changes in the operational situation. IO must be coordinated at all levels.

Just as detailed analysis is the basis for effective IO planning, operational synchronization and timing are the basis for effective IO execution. Thorough OPORD development is essential.

Because IO is multi-disciplined, it is found in various portions of the MAGTF OPORD. See also CJCSM 3122.03, *Joint Operation Planning and Execution System Volume II, Planning Formats and Guidance*. The disciplines of IO are included as tabs to the Appendix 3 (IO) to the OPORD and in the OPORD annexes for communication and information systems, PA, CMO, information management, and special technical operations.

Transition

Transition is the orderly handover of a plan or order as it is passed to those tasked with execution of the operation. It provides those who will execute the plan or order with the situational awareness and rationale for key decisions necessary to ensure there is a coherent shift from planning to execution.

The IO cell remains intact during the transition from planning to execution, and continues to support both current and future operations. The IO cell assists in the transition briefings for the remainder of the staff and subordinate commands to ensure that the IO portions of the order are known and understood. If drills are held, then the IO cell will assist as necessary. Finally, during the confirmation brief, the IO cell will ensure that the IO capable units address their tasked IO actions as part of their overall plan to identify any remaining discrepancies or gaps in planning.

Transitioning from Planning to Battle Rhythm

Having completed the MCPP steps and arrived at an executable COA, the MAGTF will be challenged to monitor the execution of the IO plan and make changes consistent with evolving operations. The IO planning process is useful in providing IO support to the steps of the MCPP (see figure 2-3 on page 2-10), defensive, and informational IO planning, and can help the MAGTF to develop the essential building blocks as follows:

- Stated IO goals and objective (based on desired operational effect).
- An IO synchronization matrix that links mutually supporting IO actions. See appendix B.
- An integrated target list.
- Approved messages and themes to guide perception management activities.

These building blocks help sustain on-going IO. Sustained IO are supported by the MAGTF intelligence cycle, BDA cycle, targeting cycle, and the MAGTF operations battle rhythm. Taken together, these processes allow the MAGTF to gather and analyze information (intelligence cycle), assess the functional capability (or destruction) of enemy C2 nodes (BDA cycle), re-attack as necessary to maintain suppression of enemy C2 (targeting cycle), and modify and issue changes to on-going plans (operations battle rhythm). It is the integration of these cycles that determines the daily IO battle rhythm. The logical transition from IO planning to the IO battle rhythm is illustrated in figure 2-4 on page 2-10.

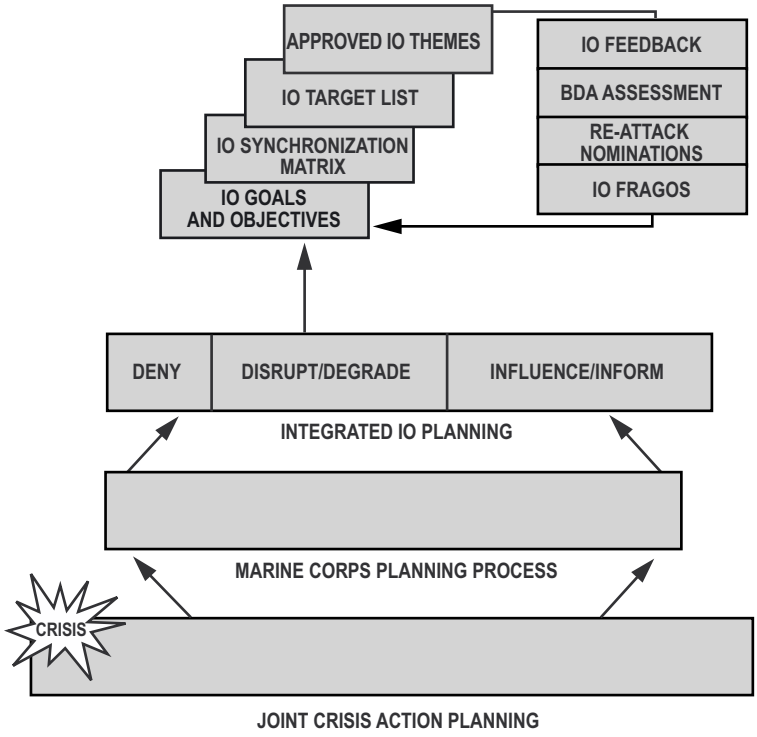

Figure 2-3. The MCPP and Integrated IO Planning.

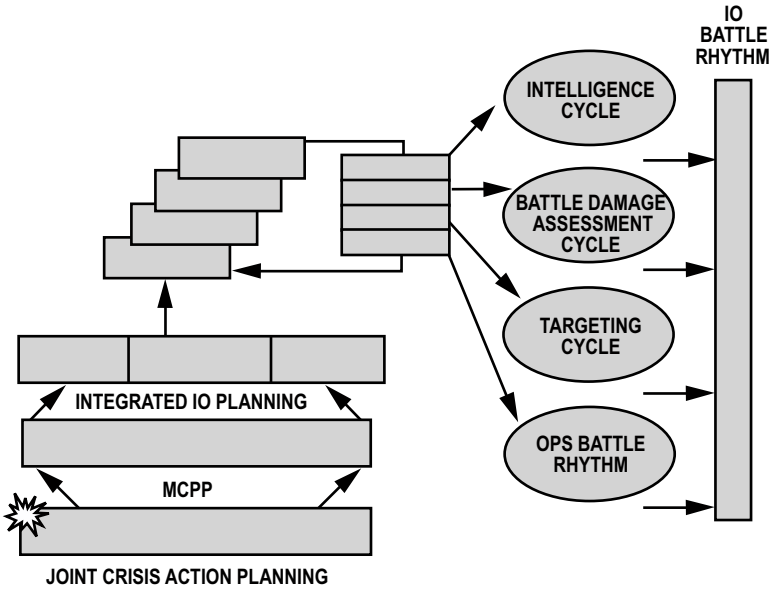

Figure 2-4. Transitioning from Information Operations Planning to Information Operations Battle Rhythm.

CHAPTER 3
INFORMATION OPERATIONS CAPABILITIES

"The means of war is force, applied in the form of organized violence. It is through the use of violence, or the credible threat of violence, that we compel our enemy to do our will."

MCDP 1, *Warfighting*

Overview

IO are multi-disciplined and a variety of elements must be employed together within an integrated strategy. Some of these elements are more offensive, defensive or informational in nature, but it is their integration into the concept of operation that ensures successful employment of IO in support of the MAGTF.

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

Information warfare (IW) is the conduct of IO during a time of crisis or conflict to achieve or promote specific objectives over a specific adversary. There is no other difference in scope or method between IW and IO.

Integration of IO is an essential part of MAGTF operations in expeditionary and joint environments. IO can mitigate the effects crisis and can help prevent or resolve conflict. When deterrence fails, IO help Marines win in war by providing essential protection and enhancing the effective use of force. IO enhance the operational capability of the MAGTF through employment of a wide range of organic capabilities, e.g., EW, OPSEC, deception, CMO, IA, PA) and by leveraging joint capabilities, e.g., PSYOP.

Deception

Description

Military deception targets enemy decisionmakers by targeting their intelligence collection, analysis, and dissemination systems. Deception requires a thorough knowledge of adversaries and their decisionmaking processes. Military deception is focused on achieving a desired behavior, not simply to mislead. The purpose is to cause adversaries to form inaccurate impressions about friendly force capabilities or intentions by feeding inaccurate information through their intelligence collection or information assets. The goal is to cause the adversary to fail to employ combat or support units to their best advantage.

Military deception operations depend on an integrated effort by all warfighting functions to create a believable story. Intelligence operations identify appropriate deception targets, assist in developing a credible story, identify and focus on appropriate targets, and assess the effectiveness of the military deception plan. Military deception operations are a powerful tool, but are not without cost. Forces and resources must be committed to the deception effort to make it believable, possibly to the short-term detriment of some other aspects of the operations. Feasible COAs rejected during planning can be particularly effective as the basis for military deception operations.

Definition

Military deception operations are 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 (JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*):

- *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.
- *Operational military deception.* Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations.
- *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.
- *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.
- *Military deception in support of operations security.* 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.

Types of Deception Operations

A deception operation may contain one or more of the following: a feint, demonstration, ruse or display.

- A *feint* is a limited objective attack that involves contact with the enemy. A feint is conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action. Feints may: (1) vary in size from a raid to a supporting attack, (2) occur before, during, or after the main attack, and (3) may be independent of the main effort. Feints may be employed to cause the enemy to react in one of three predicable ways: employ his reserves improperly, shift his supporting fires, and reveal his defensive fires.
- A *demonstration* is an attack or show of force on a front where a decision is not sought, made with the aim of deceiving the enemy. A demonstration differs from a feint in that no contact with the enemy is intended.
- A *ruse* is a trick of war to place false information in the enemy's hand. Ruses are generally single, deliberate actions. It may be necessary to group several ruses together to ensure credibility of a deception story. Ruses are extremely susceptible to detection because of inconsistency and may present the enemy with a windfall of information that he is inclined to reject.
- A *display* is a static portrayal of an activity force or equipment intended to deceive the enemy's visual observation. Displays are simulations, disguises or portrayals that project to the enemy the appearance of objects that do not exist or appear to be something else. Displays include simulations, disguises, decoys, and

dummies. They may include the use of heat, smoke, electronic emissions, false tracks, and fake command posts.

Deception in Support of the Offense

The adversary commander is the target for military deception in support of the offense. Goals may include the following:

- Achieve surprise.
- Preserve friendly forces, equipment, and installations from destruction.
- Minimize a physical advantage the enemy may have.
- Gain time.
- Cause the adversary to employ forces, including intelligence, in ways that are advantageous to the MAGTF.
- Cause the adversary to reveal strengths, dispositions, and future intentions.
- Influence the adversary's intelligence collection and analytical capability.
- Condition the adversary to particular patterns of friendly behavior that can be exploited at a time chosen by the MAGTF.
- Cause the adversary to waste combat power with inappropriate or delayed actions.

Deception in Support of the Defense

Military deception can help protect the MAGTF from adversary offensive IO efforts. Deception that misleads an adversary about friendly C2 capabilities or limitations contributes to friendly protection. An adversary commander who is deceived about friendly C2 capabilities and limitations may be more likely to misallocate resources in his effort to attack or exploit friendly C2 systems.

Operations Security and Deception

OPSEC and deception have much in common. Both require the management of indicators. OPSEC is used to deny information. OPSEC seeks to limit an adversary's ability to detect or derive useful information from his observations of friendly activities. Deception is used to feed information. Deception seeks to create or increase to the likely detection of, certain indicators that the enemy can observe and that will cause an adversary to derive an incorrect conclusion. In short, OPSEC is used to hide the real and deception is used to show the fake.

The Deception Planning Process

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

Step 1. Deception Mission Analysis

Deception mission analysis is conducted as part of overall mission analysis that is performed by the MAGTF following receipt of a new mission.

Step 2. Deception Planning Guidance

After mission analysis, the commander issues planning guidance to the staff. In addition to other planning guidance, the commander states the deception objective for the operations.

Step 3. Staff Deception Estimate

- The deception estimate is conducted as part of the operations estimate.
- Deception COAs are developed that restate the deception objective, identify the deception target and desired perception, and outline a deception story with potential deception means.
- COA strengths and weaknesses are analyzed.

Step 4. Commander's Deception Estimate

The MAGTF commander selects an operational deception COA for OPLAN development and issues any additional guidance.

Step 5. Deception Plan Development

Developing the complete deception plan is the most time-consuming part of the deception planning process. The five major actions in this step are as follows:

- Complete the deception story.
- Identify the deception means.
- Develop the event schedule.
- Identify feedback channels.
- Develop the termination concept.

Step 6. Deception Plan Review and Approval

The MAGTF commander reviews and approves the completed deception plan as part of the normal OPLAN review and approval process. Need-to-know criteria remain in effect and only a limited number of personnel will participate in this step.

Special Considerations for Deception Planning

Classification

Due to the sensitive nature of deception operations, deception planning is restricted to those personnel who have a strict need-to-know. Deception operations depend on the knowledge and utilization of enemy intelligence collection systems to deliver a deception story to an adversary. Compromise of friendly knowledge of enemy intelligence systems would be harmful and could have far-reaching strategic and operational effects.

Unintended Effects

Third parties, e.g., neutral or friendly forces not aware of the deception, may receive and act upon deception information that is intended for the enemy. Deception planners should minimize the risk to other parties.

Responsibilities

The G-3/S-3 has primary responsibility for deception. Normally, a deception officer is appointed and is responsible to the G-3/S-3 for deception planning and oversight.

Deception and the Operation Order

Tab A to Appendix 3 (IO) of Annex C (Operations) of the OPORD is the deception tab. This tab implements the recommended COA for deception. It details the specific deception tasks to be performed and specifies coordinating instructions for the control and management of deception missions.

Electronic Warfare

Definitions

Electronic Warfare

Electronic warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or the attack the enemy. The three major subdivisions within EW are: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). (JP 1-02)

Electronic Attack

Electronic attack is that division of EW involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: (1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and

electromagnetic deception, and (2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (i.e., lasers, radio frequency weapons, particle beams). (JP 1-02)

Electromagnetic Jamming

Electromagnetic jamming is the deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. (JP 1-02)

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 electronic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. (JP 1-02) Among the types of electromagnetic deception are: manipulative electromagnetic deception, simulative electromagnetic deception, and imitative electromagnetic deception.

Directed-Energy Weapon

Directed-energy weapon is a system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel. (JP 1-02)

Antiradiation Missile

An antiradiation missile is a missile which homes passively on a radiation source. (JP 1-02) These missiles use the electromagnetic emissions of a target for terminal guidance.

Electronic Protection

Electronic protection is that division of EW involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability. (JP 1-02)

Electronic Warfare Support

ES is that division of EW involving actions tasked by, or under direct control of, an operational commander, to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated 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. ES data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 1-02)

Marine Corps Electronic Warfare Organizations

The Marine Corps has two types of EW units: the radio battalion (RadBn) and the Marine tactical electronic warfare squadron (VMAQ).

The RadBn provides COMSEC monitoring, tactical signals intelligence (SIGINT), EW, and special intelligence (SI) communications support to the MAGTF. The two radio battalions are 1st RadBn located at Kaneohe Bay, HI, and 2d RadBn located at Camp Lejeune, NC. The role and structure of the RadBn continue to evolve with digital network exploitation emerging as a critical functional area. Additionally, the 3d RadBn is planned for activation in Camp Pendleton, CA, during FY04.

VMAQs provide EW support to the MAGTF and other designated forces. The VMAQ conducts tactical jamming to prevent, delay or disrupt the detection and tracking of enemy early warning, acquisition, fire or missile control, counterbattery, and battlefield surveillance radars. Tactical jamming also denies or degrades enemy communication capabilities. In addition, the VMAQ conducts

electronic reconnaissance and electronic intelligence operations. There are four VMAQs (designated VMAQ-1 through VMAQ-4) assigned to MAG-14, 2d MAW, Cherry Point, NC. Each squadron has five EA-6B Prowler aircraft.

Responsibilities

EW is the responsibility of the G-3/S-3. An EWO is normally appointed who is responsible for planning, coordinating, and tasking EW operations and activities. Other responsibilities include the following:

- Coordinate with the G-2/S-2 to establish priorities between EW and signals intelligence missions.
- Coordinate with the G-6/S-6 to facilitate maximum use of the electromagnetic spectrum through electronic protection and minimizing electromagnetic interference.

The Electronic Warfare Coordination Cell/ Information Operations Cell

The electronic warfare coordination cell (EWCC) is a dedicated EW planning cell that may be established to coordinate EW activities. The IO cell may perform functions of the EWCC if one is established.

The MAGTF commander will normally plan, synchronize, coordinate, and de-conflict EW operations through the EWCC or an IO cell. Each facilitates coordination of EW operations with other fires and communications and information systems. These centers coordinate efforts by the G-2/S-2, G-3/S-3, and G-6/S-6 to eliminate conflicts between battlespace functions. The EWCC or IO cell is under staff cognizance of the G-3/S-3. Assigned personnel identify and resolve potential conflicts in planned operations. The EWCC or IO cell includes an EWO, a communications and information systems representative, and other liaison officers as needed. Liaison could include RadBn representation, airborne electronic countermeasures officers, a Marine air control group radar officer, and other Service representatives.

MAGTF staffs will provide personnel to incorporate an EWCC or IO cell with the Marine Expeditionary Force (MEF) G-3/S-3. Personnel will also be provided for liaison teams to higher headquarters EW coordination organizations when required, such as the joint commander's electronic warfare staff (JCEWS) or JTF IO cells created by JTFs.

Electronic Warfare and the Operation Order

Tab B to Appendix 3 (IO) of Annex C (Operations) of the OPORD is the EW tab. It details specific EW tasks to be performed and specifies coordinating instructions for the control and management of EW missions.

Specific instructions for SIGINT is contained in Appendix 2 to Annex B (Intelligence). Defensive information warfare operations (IW-D) are contained in Tab G to Appendix 3 (IO) 0to Annex C (Operations). IA activities are contained in Appendix 1 to Annex K (Communication and Information Systems).

Operations Security

Description

OPSEC is the key to information denial. It gives the commander the capability to identify indicators that can be observed by adversary intelligence systems. These indicators could be interpreted or pieced together to derive critical information regarding friendly force dispositions, intent, and/or COAs that must be protected. The goal of OPSEC is to identify, select, and execute measures that eliminate or reduce indications and other sources of information, which may be exploited by an adversary, to an acceptable level.

Definition

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to (1) identify those actions that can be observed by adversary intelligence systems; (2) determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and (3) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

Operations Security in Support of the Offense

Although primarily associated with defensive measures, OPSEC contributes to the offense by depriving the enemy of information—slowing the enemy's decision cycle thereby providing opportunity attainment of friendly objectives.

Operations Security in Support of the Defense

The overall goal of OPSEC is denial and the establishment of essential secrecy. The key element that OPSEC protects is the commander's concept of operation. A good OPSEC plan denies information to the enemy intelligence system, reducing its ability to orient combat power against friendly operations.

The Operations Process

OPSEC planning is accomplished through the OPSEC process. The OPSEC process has the following five distinctive steps that provide a framework for the systematic identification, analysis, and protection of information necessary to maintain essential secrecy. (See JP 3-54, *Operations Security*)

- Identification of critical information.
- Analysis of threats.
- Analysis of vulnerabilities.
- Assessment of risk.
- Application of appropriate OPSEC measures.

Responsibilities

The G-3/S-3 has primary responsibility for OPSEC. Normally, an OPSEC officer is appointed and is responsible to the G-3/S-3 for OPSEC planning and oversight. In joint operations, an OPSEC working group may be established to recommend OPSEC measures, coordinate or conduct OPSEC surveys, and write the OPSEC portion of the OPORD.

Operations Security Support Agencies

Counterintelligence/Human Intelligence Teams

CI/human intelligence (HUMINT) teams perform a wide range of duties such as security briefings, countersabotage, counterespionage, and countersurveillance inspections. CI measures enhance security, aid in reducing risks to a command, and are essential in achieving operational surprise during military operations. CI can provide a significant contribution to a unit's OPSEC program. CI personnel can support a command's OPSEC program by the following:

- CI surveys.
- Physical security evaluations.
- Security inspections.
- Vacated command post inspections.
- Penetration inspections.
- Security education.

There is a CI/HUMINT company located within the intelligence battalion. (See MCWP 2-14, *Counterintelligence*)

Imagery Interpretation Platoon

These units interpret overhead imagery and explain the signature that a unit reveals to adversary imagery systems. This type of product requires coordination through the G-2/S-2 and sufficient lead-time to obtain. A comprehensive OPSEC plan would ideally incorporate friendly imagery support to assist in the maintenance and improvement of OPSEC measures.

Naval Criminal Investigative Service

The Naval Criminal Investigative Service (NCIS) operates a worldwide organization to fulfill the investigative and CI responsibilities of the Department of the Navy. Within this charter, the NCIS has exclusive jurisdiction in matters involving actual, potential or suspected espionage, sabotage, and subversion including defection. In a combat environment, this CI jurisdiction is assigned to Marine CI, assuming that NCIS assets are not locally available.

Operations Security and the Operation Order

Tab C (OPSEC) to Appendix 3 (IO) of Annex C (Operations) of the OPORD is the OPSEC tab. This tab implements the recommended COA for OPSEC. It details specific OPSEC tasks to be performed and specifies coordinating instructions for the control and management of OPSEC tasks.

Psychological Operations

Description

At the strategic level, PSYOP may take the form of political or diplomatic positions, announcements or communiques. At the operational level, PSYOP can include the distribution of leaflets, radio and television broadcasts, and other means of transmitting information that provides information intended to influence a selected group. It may be used to encourage enemy forces to defect, desert, flee, surrender or take any other action beneficial to friendly forces. At the tactical level, PSYOP include face-to-face contact and the use of loudspeakers or other means to deliver PSYOP messages. PSYOP shape attitudes and influence behavior. The mere presence of Marine Corps forces may be a PSYOP activity in itself, bringing influence on a situation through a display of purpose. PSYOP may support military deception operations.

Definition

Psychological operations are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. (JP 1-02). See also MCWP 3-40.6 (formerly FMFM 3-53), *Psychological Operations*.

Psychological Operations Integration

PSYOP is only one of the means available to influence enemy attitudes and behaviors. IO must broadly coordinate PA (the delivery of the truth), OPSEC (protection of friendly critical information), concealment and deception (creation of misleading perceptions), along with PSYOP (influencing people by conveying selected information).

Organization

The Marine Corps has no dedicated PSYOP units. If requested, external PSYOP support may be provided by the US Army's 4th Psychological Operations Group (POG).

Employment

During peacetime, PSYOP activities that support combatant commanders take the form of overt peacetime PSYOP programs. These programs are proposed by combatant commanders through the chairman of the joint chiefs of staff who, in turn, refers them to the assistant secretary of defense for special operations and low intensity conflict for review and approval. During contingencies, a PSYOP concept plan that is broad in scope is forwarded from the combatant commander to the joint staff for approval of overarching themes, objectives, and guidance, but not products. Once the concept plan is approved, a more detailed theater PSYOP plan is developed.

Approval authority for PSYOP may be maintained by the combatant commander or the JFC. MAGTF PYSOP actions must complement and support ongoing theater and joint force PSYOP activities.

The MAGTF will not normally identify, plan or execute complex PSYOP; e.g., those requiring detailed theme development, intricate target analysis or the use of sophisticated media. These missions will typically be conducted by external PSYOP units; e.g., US Army 4th POG, US Navy Fleet Tactical Readiness Group, US Air Force 193d Special Operations Group. However, the MAGTF commander is responsible for providing PSYOP support and conducting tactical PSYOP (primarily through words and actions) in support of the MAGTF's mission. The presence and actions of Marines on the battlefield has an inherent psychological impact on the enemy. Marines execute observable actions that support psychological objectives.

The enemy is likely to employ PSYOP to influence the local populace, attempt to weaken the political and military will of US forces, and degrade the US and world community support for military action. MAGTF counteractions should be tailored to limit the enemy's opportunities to exploit the presence of Marines and their actions for PSYOP purposes. Behavior may generate either negative or positive support from the local population. Detailed knowledge of the host nation's culture and individual self-discipline is required.

PSYOP may be integrated as a nonlethal fire support asset. PSYOP is planned by the G-3/S-3 and coordinated with PA and CMO.

Responsibilities

Overall responsibility for the conduct of PSYOP falls under the cognizance of the G-3/S-3. A PSYOP officer is provided for at the MEF G-3 future operations section. If not on-hand within the MAGTF, a PSYOP officer may be appointed to provide control and management of the PSYOP effort and to meet liaison requirements.

Psychological Operations Support Agencies

Contingency operations that require the activation of a JTF normally require the formation of a joint PSYOP task force (JPOTF). When established, the JPOTF is responsible for planning and supervising the joint PSYOP effort. The JPOTF is subordinate to the combatant commander or the JTF J-3. Liaison between Marine units serving as the Marine Corps force component of the JTF and the JPOTF is required.

The Army has the preponderance of PYSOP assets within the Department of Defense (DOD). There is one active component POG (4th POG, Ft Bragg, NC) with a worldwide capability and three reserve component POGs. A MAGTF serving as a JTF could result in 4th POG directly supporting the MAGTF.

The Air Force's 193d special operations group of the Pennsylvania National Guard flies the EC-130E Volant Solo. It provides an airborne radio and TV broadcast capability.

The Navy's fleet tactical readiness group provides equipment and technical maintenance support to conduct civil radio broadcasts and jam within radio frequency bands.

Psychological Operations and the Operation Order

Tab D (PSYOP) of Appendix 3 (IO) to Annex C (Operations) of the OPORD is the PSYOP Tab. This tab implements the recommended COA for PSYOP. It details specific PSYOP tasks to be performed and specifies coordinating instructions for the control and management of PSYOP missions.

Computer Network Operations

Description

The three basic elements of C2 are information management, people, and C2 support. CNO support C2 by facilitating the decisionmaking process by providing communication and information systems that are reliable, secure, timely, and flexible. CNO protect information and information processes through computer network defense and IA activities. CNO may also be used to attack or exploit an adversary's information systems through computer network attack or exploitation. The Marine cryptologic support battalion or the RadBn may be tasked to support CNO activities. While the MAGTF does not have a computer network attack (CNA) force, it must be aware of available joint capabilities. Additionally, the MAGTF must be prepared to defend against the CNA threat posed by the adversary. Additional guidance on CNA is available in the classified appendix A ("Supplemental Information Operations Guidance") to JP 3-13, *Joint Doctrine for Information Operations*.

Definitions

CNO are comprised of CNA, computer network defense (CND), and related computer network exploitation (CNE) enabling operations. (Director of Central Intelligence Directive [DCID] 7/3)

Computer Network Attack

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 1-02)

Computer Network Defense

Computer network defense is defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. (JP 1-02)

Computer Network Exploitation

Computer network exploitation is intelligence collection and enabling operations to gather data from target or adversary automated information systems (AIS) and networks. (DCID 7/3)

Responsibilities

CNO encompass a broad range of mutually supporting staff functions. Key staff elements include the MAGTF G-2/S-2, G-6/S-6, and G-3/S-3. Additionally, the MAGTF information management officer, information security manager, special security officer, and information systems security officer perform important supporting functions.

Operation Order

Several appendices of the OPORD relate to CNO: Appendix 1 (Information Systems Security) to Annex K (Communication and Information Systems) and Appendix 2 (IW-D) to Annex K. Annex B, Intelligence of the OPORD is the basic intelligence annex and contains elements related to CNE; i.e., Tab A (Communications Intelligence Collection Requirements) to Appendix 2 (Signals Intelligence).

Physical Attack

Description

Physical attack applies friendly combat power against the enemy. It reduces enemy combat power by destroying enemy forces, equipment, installations, and networks. Within IO, physical destruction is the tailored application of combat power to achieve desired operational effects.

ROE play a major role in determining if destruction is a viable option during a particular phase of the operation. Target planners may use physical destruction against both the C2 portions of the enemy's C2 system. However, the enemy may be able to recover from physical destruction given

sufficient time, resources, and redundancy. Planners should have some preplanned measure of effectiveness to judge the results of physical destruction, and be prepared to monitor targets after attack to determine their operational status. Critical enemy C2 nodes identified as effectively reconstituted should be considered for re-attack if analysis determines that they are still operationally effective. IO integration with the BDA cycle is essential.

As an integrated part of IO, physical attack considers the systematic degradation or destruction of selected enemy C2 systems to allow the MAGTF to gain an informational advantage. C2 nodes must be functionally destroyed. A C2 node may be operational despite cosmetic structural damage. The enemy may also be able to reconstitute C2 nodes and re-establish effective C2 via alternate means. C2 targets may need to be attacked in depth to achieve desired effects. Restrike may be required to maintain suppression of enemy C2.

The total destruction of the hostile C2 system may not be attainable or desirable. Friendly forces may need to use enemy C2 systems during the post-conflict phase of military operations. The careful selection and prioritization of C2 physical destruction targets build the strongest case when competing against other type missions for weapons and delivery platforms. See also MCWP 3-16, *Fire Support Coordination in the Ground Combat Element*.

Definition

Physical attack is defined as the application of combat power to destroy or neutralize enemy forces and installations. It includes direct and indirect fires from ground, sea, and air platforms. It also includes direct actions by special operations forces.

Target Nomination

IO planners should use the nomination and review process to ensure that IO-related targets are included on the target list. Above all, IO targets must be presented as a cohesive, integrated, and relevant target set that supports operational requirements. For example, when planning suppression of enemy air defenses, strikes against enemy C2 systems should be coordinated with strikes against enemy EW systems and command authorities. Alternatively, if planning to isolate enemy forces, strikes against C2 systems and information systems should be coordinated with strikes against lines of communication.

Nodal Analysis

IO planners should conduct a nodal analysis of enemy C2 systems prior to nominating targets. C2 targets should be selected based on their criticality to the enemy and the role they play in linking hostile C2 systems together in a network. Striking key nodes has greater effect than striking individual C2 elements and provides for economy of force thus reducing sorties flown or rounds expended and reducing friendly exposure to hostile fire.

Intelligence Gain/Loss Analysis

Some enemy C2 elements may be of such intelligence value that it is best not to destroy the target, but rather to exploit it through SIGINT or other means. Some enemy C2 systems may provide a unique and irreplaceable source of intelligence. This can only be determined by conducting an intelligence gain/loss analysis.

No-strike Target List

Equally important to the target list is the no-strike target list. Recommendations to this list should include nodes identified during intelligence gain/loss analysis. Also, those organizational or media elements that are hostile to the enemy regime and friendly to US forces should be identified. Friendly radio/TV broadcast facilities may be placed on a no-strike target list. Finally, the IO planner should consider preserving infrastructure that will be of value once US forces are ashore or to support post-conflict operations.

Timing

Physical attack should be planned to support friendly operational maneuver. After a strike the enemy may have only a short window of vulnerability before reconstituting C2 systems or establishing alternate communication paths. Physical attack should be timed for just before the adversary critically needs a C2 function to preclude timely reconstitution.

Feedback

BDA analysis is essential to determine effectiveness of physical attack efforts. For enemy C2 targets, imagery provides visual cues to destruction and should be compared with other intelligence sources, such as SIGINT and HUMINT.

Physical Attack and the Operation Order

Tab E (Physical Attack/Destruction) of Appendix 3 (IO) to Annex C (Operations) of the OPORD is the physical attack/destruction tab. This tab implements the recommended COA for attack. It details specific IO-related attack tasks to be performed and specifies coordinating instructions for the control and management of IO-related attack missions if required.

Information Assurance

Description

Marines depend on information to plan operations, deploy forces, and execute missions. While information and information systems enable and enhance warfighting capabilities, they are also vulnerable to attack and exploitation and must be protected.

Definitions

IA is information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP-02). IA capabilities include information security.

Information Security

Information security is the information security the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. (JP 1-02)

Computer Security

Computer security is the protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02)

Communications Security

COMSEC is 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. (JP 1-02) COMSEC includes cryptosecurity, transmission security, emission security, and the physical security of COMSEC materials and information.

Defense in Depth

The primary method for protecting information and information systems is through defense in depth. To prevent potential breakdown of barriers and invasion of the innermost (or most valuable) part of the system, defenses must be constructed in successive layers and safeguards positioned at different locations. These different locations may include local computing

networks, enclave boundaries, networks, and supporting infrastructures. Use of a deliberate risk analysis process can ensure that the most effective defense in depth strategy is employed given the resources available.

Education, Training, and Awareness

A key component for success in information protection is education and training of information and information system users, administrators, managers, engineers, designers, and requirements developers. Awareness heightens threat appreciation and the importance of adhering to protective measures. Education provides the concepts and knowledge to develop appropriate technologies, policies, procedures, and operations to protect systems. Training develops the skills and abilities to mitigate system vulnerabilities, and implement and maintain protected systems.

Training and Certification

Headquarters, USMC, C4 oversees the Marine Corps IA certification program. This program is based on the Computer Security Act of 1987 (Public Law 100-235) that requires "*Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation 1of each Federal computer system within or under the supervision of that agency*."

All Marines, Marine Corps civilian employees, and contractor personnel who perform Marine Corps duties as system administrators will be certified as a level 1, 2 or 3-system administrator. Once all requirements have been met by the system administrator for certification at a specific level, a "System Administrator IA Certificate" can be awarded.

System Certification and Accreditation

All DOD information systems and networks will be certified and accredited in accordance with DOD Instruction (DODI) 5200.40, *DOD Information Technology Security Certification and Accreditation Process*. Certification and accreditation of information systems that process top secret sensitive compartmented information will comply with the requirements of DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems*.

Risk Management

Risk management decisions determine limits for applying countermeasures. Risk management includes consideration of information needs, the value of the information at risk, system vulnerabilities, threats posed by adversaries and natural phenomena, and resources available for protection and defense. Once discovered, procedures and actions to minimize loss or degradation of information are also an important part of risk management.

Responsibilities

Overall responsibility for the conduct of IA falls under the cognizance of the G-6/S-6. Defensive IO include other supporting functions such as OPSEC and therefore are the responsibility of the G-3/S-3.

Information Assurance Support Agencies

The Marine Corps Information Technology and Network Operations Center (MITNOC) is located in Quantico, VA. The MITNOC provides continuous, secure, global communications; and operational sustainment and defense of the Marine Corps enterprise network (MCEN) for Marine Corps forces worldwide to facilitate the exchange of information across the defense information infrastructure.

The MITNOC exists to supply customer support to the MCEN and maintains a 24/7 helpdesk.

Reporting a virus hit or a threatening attempt to access a system is crucial. When a virus or attempted compromise occurs, the local information system security officer is contacted to obtain immediate assistance. Initial reports are initiated according to the local/regional base or station's guidance. At minimum, the MITNOC helpdesk is contacted to report the incident.

The attempt on a Marine system could be part of a larger, overall attempt to disrupt or exploit Marine information systems, and this can only be discovered and defended against if all attempts are reported.

The Service computer emergency response team for the Marine Corps is the Marine computer emergency response team (MARCERT), which is an element of the MITNOC located in Quantico, VA. The MARCERT provides real-time, 24-hour observation of the MCEN for network and host-based intrusion incidents based upon specified criteria. Valid incidents are analyzed from strategic and operational perspectives for impact upon the MCEN. This data is also warehoused to provide Marine force computer network defense with usable information to perform incident profiling, trend analysis, and predictive analysis. The MARCERT provides guidance and support to Marine Corps organizations' vulnerability testing and malicious code incident response teams.

The Joint Task Force on Computer Network Operations (JTF-CNO) serves as the focal point within the DOD to organize a united effort to defend computer networks and systems. It monitors incidents and potential threats to DOD systems and establishes links to other federal agencies through the National Infrastructure Protection Center. When attacks are detected, JTF-CNO is responsible for DOD-wide recovery operations to stop or contain damage and restore network functions to DOD operations. JTF-CNO is co-located with, and supported by, the Defense Information Systems Agency (DISA) to take advantage of the existing operational computer network capabilities of DISA's Global Operations and Security Center.

The Marine component to the JTF-CNO is the Marine Corps Forces Information Network Operations (MARFOR-INO), which is collocated with the MITNOC at Quantico, VA. The MARFOR-INO is responsible for the defense of the MCEN and other Marine Corps computer networks connected to the defense information infrastructure from strategic computer network attacks and other CND missions as directed by the JTF-CNO. The MARFOR-INO is responsible for the collection of data on CNA against the MCEN and other Marine Corps computer networks, formulating COAs to thwart CNAs, coordinate and direct actions for defense, and prioritize recovery actions.

DISA operates a program known as the DISA Vulnerability Analysis and Assistance Program specifically focusing on AIS vulnerability. Upon customer request, this program collects, identifies, analyzes, assesses, and resolves information security (INFOSEC) vulnerabilities.

The National Security Agency has a COMSEC monitoring program that focuses on telecommunication systems using wire and electronic communications.

The INFOSEC program management office is a joint DISA and National Security Agency organization charged with the execution of the defense INFOSEC program. The primary responsibility of the joint program office is to assure the effective and coherent application to the overall defense information system, and its individual component parts: the defense information system network, the defense integrated secure network, the defense data network, the defense message system, the interoperable tactical/strategic data network, and the defense data centers.

Information Assurance and the Operation Order

Appendix 1 (Information Systems Security) to Annex K (Communications and Information Systems) of the OPORD is the IA appendix. Defensive IO is addressed in Appendix 2 (IW-D) to Annex K. These appendices implement the recommended COA for IA and defensive IO. They detail specific tasks to be performed and specify coordinating instructions for the control and management of IA and defensive IO.

Physical Security

Description

Physical security contributes directly to information protection. Information, information-based processes, and information systems—such as C4 systems, weapon systems, and information infrastructures—are protected relative to the value of the information they contain and the risks associated the compromise or loss of information.

Definition

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 1-02)

Responsibilities

In general, physical security is an operations function and is the responsibility of the G-3/S-3. However, specific measures related to the protection of information and information systems are developed and implemented by the G-6/S-6.

Operation Order

Tab B (Physical Security) to Appendix 15 (Force Protection) of Annex C (Operations) of the OPORD is the physical security tab. However, physical security activities related to the protection of information may also be included in Appendix 1 (Information Systems Security) or Appendix 2 (Defensive Information Warfare) to Annex K (Communication and Information Systems) of the OPORD.

Counterintelligence

Description

The principal objective of CI is to assist with protecting friendly forces. CI is the intelligence function concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion or terrorism. CI enhances command security by denying adversaries information that might be used against friendly forces and to provide protection by identifying and neutralizing espionage, sabotage, subversion or terrorism efforts. CI provides critical intelligence support to command force protection efforts by helping identify potential threats, threat capabilities, and planned intentions to friendly operations while helping deceive the adversary as to friendly capabilities, vulnerabilities, and intentions. Combating terrorism makes us a less lucrative target. CI increases uncertainty for the enemy, thereby making a significant contribution to the success of friendly operations. CI also identifies friendly vulnerabilities, evaluates security measures, and assists with implementing appropriate security plans. Physical security reduces vulnerability. OPSEC reduces exposure. The integration of

intelligence, CI, and operations culminates in a cohesive unit force protection program. See also MCWP 2-14, *Counterintelligence*.

Definition

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 1-02)

The Counterintelligence Process

The CI process at all levels is conducted by using a standard methodology that consists of four steps as follows:

- Develop a CI estimate.
- Conduct the CI survey.
- Develop the CI plan.
- Conduct CI operations and assist with implementation of CI measures.

The Counterintelligence Estimate

Included in CI estimates are known factors on location, disposition, composition, strength, activities, capabilities, weaknesses, and other pertinent information. CI estimates also provide conclusions concerning probable COAs and future activities of these organizations, effects of those activities on friendly COAs, and effectiveness of friendly force CI measures. Within the MAGTF, intelligence and CI analysts of the MAGTF command element (CE), intelligence battalion, and its CI/HUMINT company/detachment will normally prepare a tailored CI estimate that addresses threats to the MAGTF by using an IPB methodology that is focused on CI factors and the CI threat. However, each level of command must conduct its own evaluation to determine which adversary's capabilities identified in the MAGTF CI estimate represent a threat to their particular unit. The CI estimate must be updated on a regular basis, and the revised estimate or appropriate CI warning reports must be disseminated to units involved in the operation.

The Counterintelligence Survey

The CI survey assesses a unit's security posture against the threats detailed in the CI estimate. The CI survey should identify vulnerabilities to specific hostile intelligence, espionage, sabotage, subversion or terrorist capabilities and provide recommendations on how to eliminate or minimize these vulnerabilities. The survey should be as detailed as possible. During the planning phase of an operation, it may be possible to do a formal, written survey. During rapid planning, the survey will likely result from a brief discussion between the appropriate intelligence, CI, operations, communications, and security personnel. It is critical that the survey looks ahead and supports the development of the CI measures necessary for each phase of the operation.

The Counterintelligence Plan

The CI plan details the activities and operations used to counter hostile intelligence, sabotage, subversion, and terrorist threats. It includes procedures for detecting and monitoring the activities of hostile intelligence and terrorist organizations and directs the implementation of active and passive measures that are intended to protect the force from these activities. The CI plan is based on the threats identified in the CI estimate and the vulnerabilities detected by the CI survey. Included in the MAGTF CI plan are details of the employment of dedicated CI capabilities and the conduct of specialized CI operations intended to detect and neutralize or eliminate specific threats. Plans of subordinate MAGTF elements closely follow the MAGTF plan, normally adding only security measures that are applicable to their specific units.

Counterintelligence Execution

An understanding of the capability of adversarial intelligence organizations to collect information on evolving US technologies is critical to developing

appropriate countermeasures. CI personnel can obtain information from other national intelligence and security organizations through liaison arrangements. The role of CI may increase when US military operations rely upon cooperation and support of allies. CI personnel can assess the capabilities, effectiveness, organization, and methods of operation of allied intelligence information on enemy intelligence, sabotage, subversive, and terrorist organizations relevant to the current mission, situation, and area of operations.

Counterintelligence Measures

CI measures-both active and passive-encompass a range of activities designed to protect against hostile intelligence, espionage, sabotage, subversion, and terrorism threats.

Responsibilities

The unit intelligence officer plans, implements, and supervises the CI effort for the commander. The G-2/S-2 may have access to or request support from MAGTF CI units and specialists to assist in developing CI estimates and plans. Members of the command are involved in executing the CI plan and implementing appropriate CI measures. Key participants in this process and their responsibilities include the following:

- *Unit security manager*: Overall integration and effectiveness of unit security practices.
- *G-3/S-3*: Force protection, OPSEC, counterreconnaissance, and deception.
- *G-6/S-6*: Communications and information systems security.
- *G-1/S-1*: Information and personnel security.
- *Headquarters commandant*: Physical security.

Operation Order

Appendix 3 (Counterintelligence) to Annex B (Intelligence) of the OPORD is the CI appendix.

Public Affairs

Description

The PA mission is to provide timely, accurate information to Marines and the general public and to initiate and support activities contributing to good relations between the Marine Corps and the public. PA expedites the flow of accurate and timely information to internal and external audiences. In peacetime, PA provides Marine and the general public with information that increases public understanding of the Marine Corps' roles and missions. PA efforts can have positive as well as negative impacts within the battlespace and the consequences of its use can have a strategic effect on the mission.

The PA challenge is to get information out effectively, efficiently, and honestly. Marine Corps PA policy is to tell the truth as quickly as possible. That includes good news as well as bad. PA informs and educates. PA must be carefully separated from other informational efforts aimed at manipulating perceptions. Any deviations from the truth will destroy the credibility and effectiveness of Marine Corps PA operations. See MCWP 3-33.3, *Marine Corps Public Affairs*.

Definition

Public affairs are those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the DoD. (JP 1-02)

Public Affairs, Psychological Operations, and Civil-Military Operations

Coordination and staff interaction between PA, PSYOP, and CMO are required to ensure that the activities of one function do not conflict or

complicate the work of another. In an expeditionary setting, all may disseminate information to local populations. However, PA elements have the responsibility to deal with media outlets. They can assist the other functions in passing information to the public through the appropriate media outlets. However, PSYOP and CMO may use message channels that are not used by PA, such as mobile loudspeakers or leaflets, to disseminate their message.

Responsibilities

PA is a special staff function executed by the MAGTF public affairs officer (PAO).

Public Affairs and the Operation Order

Annex F (PA) of the OPORD is the PA Annex. This annex implements the recommended course of action for PA. It details specific PA tasks to be performed and specifies coordinating instructions for the control and management of PA missions, if required.

Civil-Military Operations

Description

Each military operation has a civil dimension. The civil dimension requires that commanders consider how their actions affect, and are affected by, the presence of noncombatants. Accordingly, CMO have become an integral element of military operations. Through careful planning, coordination, and execution, CMO can help the MAGTF win by shaping the battlespace, enhancing freedom of action, isolating the enemy, meeting legal and moral obligations to civilians, and providing access to additional capabilities.

CMO are applicable at the strategic, operational, and tactical levels. Marines are deployed across the globe to support regional engagement strategies. Marines further national goals through the forward presence of expeditionary units. Marines are involved in multinational training activities and exercises that contribute to international cooperation and stability. Marines respond to complex emergencies, such as natural disasters, that overwhelm civil authorities. Marines contribute to peacekeeping and peace enforcement missions and are prepared to use force and/or the threat of force to deter conflict. If efforts to preserve peace fail, Marines employ carefully focused military capability to accomplish national objectives swiftly and with as little loss of life as possible. Once hostilities are concluded, MAGTFs contribute to stabilization, recovery, and to the peaceful transition of control back to civil authorities.

In every case, Marines will operate in close contact with civilians and their governments. The need exists to carefully develop, nurture, and maintain positive relations between the people, governments, and NGOs in the area of operations. The activities that the commander undertakes to create and foster positive relations between military forces and civilians are included in CMO. Effective CMO further national goals, help military commanders meet their international obligations to civilians, and enhance the effective use of combat power.

Effective CMO maximize civilian support for, and minimize civilian interference with, the mission. There is a CMO component to each and every military operation, even though the MAGTF resources devoted to CMO will necessarily vary during particular operations and throughout the various phases of each operation. CMO are not limited to operations in which the

MAGTF provides support or services to civilians or their governments, such as humanitarian and civic assistance or disaster relief efforts. CMO are conducted to facilitate military operations, achieve military operational objectives, and satisfy US policy goals. See also MCWP 3-33.1, *MAGTF Civil-Military Operations*.

Definitions

Civil-Military Operations

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

Civil Affairs

Civil affairs is the 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 1-02)

Civil-Military Operations, Civil Affairs Forces, and Civil Affairs Activities

CA describes designated personnel and distinct units. It is neither a mission nor an objective, but the name of a particular force that helps the MAGTF commander to plan, coordinate, and conduct CMO. CA forces bring expertise that is not normally available to the MAGTF. CA forces are organized and equipped specifically to support CMO and to conduct CA activities. CA activities embrace the relationship between military forces and civil authorities, and involve the application of particular skills that are normally the responsibility of civil government. CA activities include public administration, public health, economic development, and utilities.

CMO build and use relationships with civilians and other groups to facilitate operational tasks across the full range of military operations. Any element of the MAGTF may participate in the planning and execution of CMO. Whether a Marine is an operational planner dealing with a member of a foreign government, a member of a team working with an international relief organization or a rifleman at a checkpoint talking with a local farmer, that Marine is conducting CMO. CMO occur throughout the planning and execution of military operations and are not merely an adjunct specialty that occurs before or after hostilities. CA activities, however, are distinguishable from CMO to the extent that CA activities are characterized by the application of functional specialties in areas normally the responsibility of the local government or civil authority. CA forces help the MAGTF do this.

CMO, executed by CA forces, may include performance by military forces of activities and functions normally the responsibility of local government. CMO can assist to support friendly or host-nation civilian welfare, security, and developmental programs, and can publicize the existence or success of these activities to generate target population confidence in and positive perception of US and host-nation actions. See also MCWP 3-33.1.

Types of Civil-Military Operations

CMO focus on the relationship between military forces and CA, NGOs, IOs, and populations in areas where military forces are present. While executing CMO, the MAGTF may find itself

involved in a wide variety of activities including the following:

- Population and resource control.
- Foreign humanitarian assistance.
- Military civic action.
- Nation assistance operations.
- Civil preparedness and/or emergency operations.
- Civil administration.
- Domestic support operations.

Responsibilities

CMO is a function of operations. The CA officer normally operates under the staff cognizance of the operations officer (G-3/S-3). However, in situations in which civil-military considerations are a priority, the MAGTF commander may choose to designate the CA officer as a member of the general/executive staff. When trained CA personnel are not immediately available, the commander may designate a staff member to undertake the function.

Civil-Military Operations and the Operation Order

Annex G (CMO) of the OPORD is the CMO annex. This annex implements the recommended COA for PA. It details specific CMO tasks to be performed and specifies coordinating instructions for the control and management of CMO missions, if required.

CHAPTER 4
INTELLIGENCE, COMMUNICATIONS AND INFORMATION SYSTEMS, AND INFORMATION MANAGEMENT

"Command and control is about making and executing decisions. The main purpose of intelligence is to support the decisionmaking process."

MCDP 2, *Intelligence*

"The critical thing is not the amount of information, but key elements of information, available when needed and in useful form, which improve the commander's awareness of the situation and ability to act."

MCDP 6, *Command and Control*

Intelligence

Intelligence Support to Planning

Intelligence provides the essential basis for planning IO through the following considerations:

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

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

Intelligence support to IO planning is conducted as part of the IPB process; IPB is not a product. It supports the commander's battlespace area evaluation by assisting the commander in defining the battlespace, COGs, and potential critical information requirements. One of the key outputs from IPB is an analysis of the desired objectives and/or end states. These desires are usually categorized relative to broad capabilities. The categories may be elements of national power such as politics, economics, military, and society. Capability analysis processes within IPB also provide detail on the capacity and intent to conduct or sustain IO.

IPB is the following four-step process:

- Define the battlespace environment.
- Describe the battlespace effects.
- Evaluate the adversary.
- Determine adversary potential COAs.

Intelligence support will aim to define critical nodes and vulnerabilities within the adversary's information structure, which include the key personnel, equipment, and procedures and protocols involved in the transfer of information required for successful C2. Intelligence support will help focus the OPLAN on the systematic disruption of critical information nodes and information carriers. Friendly force staff advice, linked to intelligence advice on adversary COAs and CI advice on the threats to security, provide the operational planning process with the background to decide the protective measures required for nodes and

information carriers. Accurate, timely, and directed intelligence provides the foundation on which IO are based. See also Field Manual (Army) (FM) 34-130, *Intelligence Preparation of the Battlefield*.

The Marine Corps Intelligence Activity's IO/information warfare generic information requirements handbook promulgates frequently used essential elements of information/priority intelligence requirements to facilitate rapid, time-sensitive, crisis information operations planning for the MAGTF. The IO handbook is an excellent baseline support tool for those organizations providing intelligence support to IO to forward deployed naval units.

Intelligence Support to Operations Security

OPSEC, an operations function, seeks to reduce or deny the adversary information concerning friendly dispositions, capabilities, vulnerabilities and intentions both on training and operations. The OPSEC plan may incorporate PSYOP or deception to direct the adversary's attention away from major preparations, movements or other vital parts of an operation that cannot be hidden, and EW and physical attack to counteract or destroy key adversary command, control, communications, computers intelligence, surveillance, and reconnaissance (C4ISR) capabilities. Public information activities and the media can also influence OPSEC.

Intelligence support for OPSEC planning focuses on the capabilities and limitations of the adversary's C4ISR systems, to reduce the vulnerability of friendly C2 assets and installations to attack. CI resources will be concentrated on the security threat. HUMINT, SIGINT, and imagery intelligence (IMINT) are important in assesses the effectiveness of the OPSEC plan.

Intelligence support for OPSEC planning should focus on the adversary's C4ISR capabilities, including the adversary's decision cycle and any bias towards certain information/intelligence collectors or disciplines. Key information/intelligence requirements to support OPSEC are listed in the IO handbook.

Intelligence Support to Psychological Operations

PSYOP, an operations function, aims to influence adversary attitudes and behavior, thereby affecting the achievement of military objectives. Effective PSYOP can degrade adversary C2. Intelligence provides significant input to all aspects of PSYOP.

The PSYOP staff works closely with the intelligence staff to plan PSYOP and effectively integrate these with the other IO elements. OPSEC may be essential to the PSYOP plan. Equally, it may be desirable in support of PSYOP to reveal certain aspects of friendly dispositions, capabilities, and intentions.

The Marine Corps Intelligence Activity can provide the basic psychological intelligence on the cultural, religious, social, and economic aspects of the target country/population and its government/leadership, communications, and media. Sometimes referred to as human factors analysis, this data is often compiled during peacetime. During operations, this data is supplemented by intelligence provided by the G-2/S-2.

The intelligence assessment contributes to the development of psychological assessments. The latter looks more widely to identify target audiences within the opposing force, and those factors that are most likely to influence their attitudes and behavior in favor of the MAGTF mission. The conditions and attitudes of target groups are likely to change as the situation develops. Current all-source intelligence, in particular HUMINT and SIGINT, is therefore vital in the planning phase, and then throughout the execution of PSYOP, to

assess the effectiveness of current campaigns, and to reinforce success and re-allocate limited resources, if the desired effect is not being achieved. Defensively, the intelligence staff also monitors the effect of the adversary's PSYOP on the MAGTF force. CI provides intelligence on, and can be tasked to counteract, subversion that forms part of the adversary's PSYOP campaign.

Key information/intelligence requirements both for planning and executing PSYOP and for ensuring that the adversary's PSYOP are ineffective are listed in the IO handbook.

Intelligence Support to Deception

Deception, an operations function, aims to present a deliberately false picture to the adversary to cause him to act contrary to his interests. Deception is highly complex, in particular those aspects that seek to exploit adversary C2, and it demands security at the highest level. OPSEC is essential to deception to conceal those aspects and indicators that would allow the adversary to determine the reality behind the deception.

Intelligence supports deception planners by analyzing the adversary's C4ISR capabilities and identifying his perception of the battlefield and any changes in this as the battle develops. It also includes their deception doctrine, tactics/procedures, capabilities, and intentions. This requires an insight into the adversary commander's way of thinking, including the estimate process. The psychological analysis conducted as part of the PSYOP planning process may assist in providing this.

Deception uses selected conduits, identified by intelligence, to feed information to the targeted adversary decisionmaker. EW, CNO, CI, and physical attack support deception by shaping the conduits that feed information to the targeted adversary. While the selected conduits are not targeted, other conduits with information that may degrade the deception's effectiveness and success are targeted for EA or physical attack. Intelligence must monitor and support the identification of deception conduits as well as conduits targeted with EA, CNO or physical attack.

During the execution of deception operations the adversary's response must be monitored to determine whether the deception operation is achieving its aim. In analyzing this intelligence, attention must also be paid to possible adversary deception operations. Key information/intelligence requirements to plan/execute deception operations and to reduce the effects of adversary deception actions against friendly C2 are listed in the IO handbook.

Intelligence Support to Electronic Warfare

The interception, identification, analysis, and, where possible, the understanding of the adversary's electro-magnetic table can provide early warning of adversary action and support force protection. It is especially important for IO planners to locate the adversary's C2 means, to identify his communications architecture, including his offensive EW capability, and to highlight critical/vulnerable C2 systems.

Intelligence support to EW establishes target acquisition priorities, based on the CCIR and concept for future operations. The decision to target adversary C2 must be based on an assessment of the balance between destruction, neutralization, and exploitation, and between hard-kill and soft-kill methods. It may, for example, be necessary to ensure that certain adversary EW support systems are protected from attack, in support of the electronic deception plan. Such key decisions must be made at the highest level and included in the commander's guidance. Decisions on targeting will also have to be coordinated with allies.

Key information/intelligence requirements to support EW both to degrade the adversary commander's C2 cycle and to nullify the effects of adversary EW actions against friendly C2 are listed in the IO handbook.

Intelligence Support to Physical Attack

The focus of intelligence support is to provide details of target types, locations, movement, assessment of possible collateral damage, and the capability through BDA to assess the effectiveness of targeting. There is a requirement for close integration with national targeting priorities. An assessment must also be made, with G-2/S-2 advice, on the balance of advantage of destruction against exploitation, including the development of a no-strike (both passive and active measures) targeting list. It can be equally as important to use the adversary's C2 system against him, whether through EW, deception or PSYOP, as it is to destroy all or part of it. The physical attack plan must also take account of the OPSEC plan, which may require attacks on certain adversary C4ISR assets.

Key information/intelligence requirements to support targeting/physical attack and to reduce the vulnerability of friendly C2 assets and installations to attack are listed in the IO handbook.

Intelligence Support to Computer Network Operations

CNO consist of CND, CNA, and CNE. CNE is a supporting intelligence activity governed by existing intelligence regulations and is a critical enabling activity supporting CND and CNA. The RadBn is a major contributor of intelligence information supporting CNO. All CNE efforts conducted by tactical units must be coordinated with appropriate national agencies and the IO cell of the supported and/or higher unit.

Intelligence Support to Information Assurance

A coordinated IA plan to protect friendly C2 systems from adversary attack will make an adversary's IO more difficult. Defensive IO activities must also protect the intelligence and information conduits that feed the C2 system and friendly commanders. Intelligence provides the assessment of adversary IO capability and intentions. Key information/intelligence requirements to support IA are listed in the IO handbook.

Communications and Information Systems

The rapidly changing nature of information technology is shaping the communications and information environment. Technological improvements in speed, processing power, and networking capabilities continue to compress time and space, forcing higher operating tempos and creating a greater demand for information sharing. Marine Corps communications and information systems seek to harness the potential of the on-going technical revolutions. Marine Corps communication and information systems capitalize on commercial technology-recognizing the extraordinary pace of information technology change-while preserving a common set of standards in technical architectures, information protocols, applications, and security. Deployed forces and their supporting shore infrastructure will be able to share information as never before. This information sharing and the associated information management processes will improve combat readiness and support to the warfighter, enhancing decisionmaking and collaboration among commanders, and allowing better situational awareness.

The MAGTF C4I architecture is the concept for the integration of Marine Corps tactical information systems. MAGTF C4I architecture provides commanders and their staffs at all levels of the MAGTF with the capability to send, receive, process, filter, and display data to aid them in their decisionmaking process. MAGTF C4I also provides a shared situational awareness through a common picture of the battlespace. See also MCWP 3-40.3, *Communications and Information Systems*.

Information Management

Commanders require quality information to understand situations and events and to quickly control the challenges that confront them. Quality information, that which adds value to the decisionmaking process, can determine success or failure. One of the responsibilities of the commander is to determine his information requirements. Management of this information is critical. Marine Corps unit headquarters are predominantly organized along warfighting functions. Information traditionally flows into and through the staff sections, restricted by their functional boundaries. However, the operational environment and emerging threats require force mobility and unit dispersion. The ability to simultaneously share useful information with personnel at distant locations will be required to support C2 decisions. Communication and information systems, along with careful information management, must enhance operational reach and tactical flexibility. These requirements contribute to the growing information challenge facing the MAGTF. Effective information management can deliver critically important information in a timely manner to those who need it in a form they quickly understand.

Quality information adds value to the decisionmaking process. Information is susceptible to distortion, both by the enemy (intended) and by friendly sources (unintended). In the face of uncertainty, it is important to consider information quality characteristics. See table 4-1.

Table 4-1. Information Quality Characteristics.

Accuracy	**Information that conveys the true situation.**
Relevance	**Information that applies to the mission, task or situation at hand.**
Timeliness	**Information that is available in time to make decisions.**
Usability	**Information that is in common, easily understood format and displays.**
Completeness	**All necessary information required by the decisionmaker.**
Brevity	**Information that has only the level of detail required.**
Security	**Information that has been afforded adequate protection where required.**

Information Management Principles

The following principles are required to efficiently and effectively manage information to support decisionmaking. These principles guide information management at every level of command. See also MCWP 3-40.2, *MAGTF Information Management*.

Use Requirements to Define the Information Management

Command relationships, organization of the force, and information needs influence the flow of information. Recognition of user requirements and the resulting information flow allows commands to apply the proper mix of personnel, equipment, training, and procedures and network infrastructure to produce information needed to make decisions.

Tailor Information for the Commander

Filter out unnecessary, redundant or irrelevant information according to the defined information requirements to prevent information overload. Provide information in a format that the commander has specified.

Use Multiple Sources of Information

Knowledge is normally gained from information derived from fused products. Use of multiple sources normally improves information accuracy and reduces error. Use of multiple sources also increases network traffic and can add to the delay between gathering information and gaining knowledge. There needs to be a balance between collecting, processing, and dissemination.

Deliver Information on Time

Information provided late does not support decisionmaking. When information requirements are defined, the requirements should be in sufficient detail to enable personnel to determine when the information is required.

Disseminate Accurate and Relevant Information

Inaccurate or irrelevant information is worse than no information at all. However, even fragmentary information that supports critical information requirements may be of some value, if validated and provided in a timely manner in a form that is clearly understood.

Create Flexible and Redundant Procedures and Plans

The information management plan must be able to overcome changes generated by battle damage, sudden increases in the volume of information, and the needs reflected by different commanders at all echelons of command. The information management plan should have redundant capabilities and incorporate back-up procedures, alternate paths, and primary and alternate personnel/organizations. It should avoid having any "single point of failure" anywhere in the network, security, information or IA architectures.

Protect Information through a Vigorous Security Program

Information management must assure the integrity of the information and the sources/databases from which that information was derived. Corrupted or degraded information is of little value and will adversely affect the quality of the decisionmaking process.

Considerations

Effective communications and information management must enhance decisionmaking. A principal aim of communication and information systems is to enhance the commander's ability to make sound and timely decisions. Recognizing that all decisions must be made in the face of some uncertainty, communication and information systems strive to make the right elements of information available at the right time and place.

Effective communications and information management must enhance battlespace awareness. Battlespace awareness permits the commander to make decisions with incomplete information—with less than perfect understanding. Situational awareness is a personal perspective or ability to determine the relevance of unfolding events. The two elements of situational awareness are as follows:

- *Information.* The staff and major subordinate commands provide analytical information in the form of feedback to help build the commander's understanding of the situation.
- *Skill.* The commander provides the intuitive aspect of situational awareness in order to understand the situation in the absence of complete information. This personal element of situational awareness is based on the commander's experience, education, judgment, and intuition.

The combination of information and skill provides the commander with an image of the situation from which he can base future decisions. Some level of situational awareness can be achieved with raw data. Situational awareness tends to strengthen as information higher in the information hierarchy is received. Enhanced situational awareness enables the commander to be better prepared to anticipate future conditions, visualize operations, provide guidance, and accurately assess situations. Developing accurate situational awareness with limited and uncertain information under severe time constraints is the fundamental challenge of information management.

INFOSEC must be considered. The MAGTF depends upon information to plan operations, deploy forces, and execute missions. INFOSEC must be provided to protect information and information systems. This includes protection, detection of attack on friendly systems, planning for reaction capabilities, and providing for the restoration of information systems after attack.

Protection of information is an operational issue. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (JP 1-02) Defensive IO are conducted through IA, physical security, OPSEC, counterdeception, counter-PSYOP, CI, EW, and special IO. Overall responsibility for the conduct of IA falls under the cognizance of the G-6/S-6. However, defensive IO include other supporting functions, such as OPSEC, and therefore are the responsibility of the G-3/S-3.

APPENDIX A
INFORMATION OPERATIONS CELL RESPONSIBILITIES

The IO cell is a task-organized group that may be brought together within a MAGTF and/or higher headquarters to focus the IO effort. During planning, the IO cell may be established to plan efforts among various staffs, organizations, and parts of the MAGTF staff responsible for planning the various elements of IO. During execution, the cell should be available to assist in coordination, support or adjustment of IO efforts.

The IO cell is comprised of intelligence personnel, augmentees supporting IO activities, representatives from staff elements, and subject matter experts from appropriate warfighting functions. The size and structure of the cell are tailored to the mission and the commander's intent. The IO cell should have the communications connectivity, either through the combat operations center or separately, to effectively coordinate changing IO requirements. The IO cell is responsible for the following:

- Plan the overall IO effort including preparing Appendix 3 to Annex C, Information Operations, to the MAGTF OPORD. Coordinate to ensure synchronization with Annex F (Public Affairs), Annex G (Civil Affairs), Annex K (Communications and Information Systems), Annex S (Special Technical Operations), and Annex U (Information Management).
- Develop offensive and defensive IO concepts.
- Recommend IO priorities.
- Coordinate subordinate IO plans.
- Coordinate the planning and execution of IO activities between organizations responsible for each IO element.
- Coordinate nodal analysis and compile IO target list. Submit IO targets for inclusion in MAGTF targeting plans.
- Ensure OPSEC plan provides necessary command, control, and communications protection and is coordinated with the deception plan and operations.
- Ensure other IO elements support the deception effort.
- Ensure PSYOP themes support, and are supported by, the other IO elements.
- Coordinate intelligence support to all IO elements.
- Coordinate and de-conflict IO operations with special information operations (SIO) and special technical operations (STO).
- Recommend additions, deletions, and modifications to ROE.

Information Operations Officer

- Responsible to the G-3/S-3 for all MAGTF IO.
- Responsible for preparing the IO annex to OPORD.
- Ensure IO representation and input provided to MAGTF operational planning team.
- Oversee core personnel within the IO cell and call plenary IO cell meetings that include external support augmentees as appropriate.
- Coordinate all IO matters with higher, adjacent, and subordinate units.
- Request external support from and coordinate IO activities with IO organizations such as joint information operations command, joint warfare analysis center, national security agency, defense intelligence agency, and joint COMSEC monitoring activity (JCMA).

Intelligence (G-2/S-2) Member

- Provide timely and directed intelligence support to IO.
- Advise on enemy order of battle, infrastructure or enemy commander profiles.
- Provide intelligence gain/loss analysis and reconcile restricted C2 targets on the restricted frequency list.
- Provide BDA and effectiveness feedback reporting for IO activities.
- Coordinate the development and prioritization of IO intelligence requirements.
- Identify collection requirements based on specific needs identified by the IO cell.
- Coordinate development of targeting products to support IO campaign planning.
- Coordinate the development of IO-related IPB products.
- Assist preparation of IO portions of MAGTF exercises and OPLANs.
- Inform MAGTF S-2/G-2 of IO planning or execution activity to engage appropriate intelligence, surveillance, and reconnaissance (ISR) capabilities for targeting and impact assessment.
- Notify other MAGTF staff elements of decisions made within the IO cell that have potential impact on their functional areas of responsibility.
- Provide assistance (through the IO cell) in assessing the operational impact and recommending appropriate recovery/response actions for computer intrusions affecting MAGTF computer infrastructures in support of the S-6/G-6 mission supporting IA.
- Coordinate nomination of protected frequencies for inclusion into the joint restricted frequencies list.
- In concert with IO Cell, coordinate development and prioritization of IO ISR-related requirements.
- In concert with S-3/G-3 and S/G-6, coordinate COMSEC monitoring support from the JCMA, including JCMA's own force protection communications support and the RadBns, during operations and exercises. Identify areas of OPSEC concern for JCMA and the RadBn focus. Integrate COMSEC monitoring activities with trusted agents for other IO activities; e.g., PSYOP, deception, OPSEC, and CI functions to enhance IO efforts.
- In coordination with headquarters staff representatives, identify critical MAGTF information resources outside the MAGTF area of responsibility. Prepare notification messages for supporting commands or agencies to highlight the need to monitor and protect these critical nodes.

CIS (G-6/S-6) Member

- Provide information on signal security and communication security efforts and recommend adjustments.
- Identify critical C4 nodes for defensive IO protection.
- Provide protected and restricted frequencies to the restricted frequency list.
- Coordinate and report on JCMA monitoring of MAGTF C4I architecture.

Operations Security Officer

- Oversee overall OPSEC efforts.
- Develop and update the OPSEC plan.

- Initiate an OPSEC feedback program to monitor OPSEC effectiveness.
- Coordinate all OPSEC activities with external agencies and organizations.

Psychological Operations Officer

- Maintain a thorough knowledge of all PSYOP plans and actions.
- Provide expert advice on PSYOP matters.
- Coordinate PSYOP plans, actions, and support with other IO elements, especially OPSEC and deception.

Deception Officer

- Head deception cell.
- Coordinate development and update of deception plan, including obtaining higher-level authority if required.
- Monitor and control dissemination of deception-related information; ensure security of material is maintained.
- Coordinate deception plans with other IO elements.
- Coordinate with the G-2/S-2 for feedback on deception success.
- Monitor and control execution of the deception event schedule.

Electronic Warfare Officer

- Oversee the EW coordination cell under the direction of the G-3/S-3.
- Prepare EW plans.
- Coordinate EW operations with internal units and external agencies.
- Coordinate EW operations with other IO elements.
- Establish and maintain the restricted frequency list with the G-6/S-6.

Special Information Operations/Special Technical Operations Officer

- Plan, coordinate, and de-conflict SIO/STO activities.
- Ensure the IO cell is aware of SIO/STO activities as required.
- Conduct liaison with higher SIO/STO representatives to facilitate coordination and release and execution authority for SIO/STO.

Counterintelligence Officer

- Assess defensive IO posture from a CI perspective.
- Recommend corrective actions.

Targeting Representative

- Provide entry for IO targets into the targeting cycle.
- Ensure IO targets are given proper consideration in the targeting process.
- Provide IO cell recommendations to the restricted target list.

Other Representatives

- Attend IO cell sessions as invited by IO Officer.
- Provide expert advice and opinions.
- Coordinate with parent organizations in support of MAGTF IO.

APPENDIX B
INFORMATION OPERATIONS PLANNING TOOLS

Information Operations Synchronization Matrix

The IO synchronization matrix (figure B-1) is commonly used during COA analysis to portray the time-phased aspects of IO activities. It generally presents more detail than the IO planning worksheet (figure B-2).

Time Phase					
OPSEC					
PSYOP					
EW					
Physical Destruct					
Deception					
Civil Affairs					
Public Affairs					

Figure B-1. Information Operations Synchronization Matrix.

Information Operations Planning Worksheet

During COA development, IO planners can use a planning worksheet to develop IO tasks for each COA. One worksheet is completed for each IO objective; cumulative worksheets are an outline for IO support for that COA. The IO planning worksheet helps tie together the staff products generated during scheme of maneuver development.

Concept: _____

COA: _____

Objective: _____

<table>
<tr><td>Maneuver Endstate</td><td rowspan="2">Offensive IO Targets</td><td rowspan="2">Defensive IO Targets</td></tr>
<tr><td>Destruction Tasks</td></tr>
<tr><td>EW Tasks</td><td colspan="2" rowspan="2">IO IRs</td></tr>
<tr><td>PSYOP Tasks</td></tr>
<tr><td>OPSEC Tasks</td><td colspan="2" rowspan="5">Coordination and Instructions</td></tr>
<tr><td>Deception Tasks</td></tr>
<tr><td>Civil Affairs Tasks</td></tr>
<tr><td>Public Affairs Tasks</td></tr>
<tr><td>Other Tasks</td></tr>
</table>

Figure B-2. Information Operations Planning Worksheet.

Information Operations Execution Matrix

Used during planning and execution, the IO execution matrix converts the generalities of the synchronization matrix into specific taskings and requests to IO-capable units.

IO Task	Location	Means Employed/ IO Element	Tasked Unit or System	Time	Assessment Method/Means	Remarks
Execution/Coordination Instructions:						

Figure B-3. Information Operations Execution Matrix.

APPENDIX C
INFORMATION OPERATIONS ORGANIZATIONS

Organization and Location	Description
USSTRATCOM Offutt AFB, NE	DOD lead for CND and CNA activities.
Joint Information Operations Center (JIOC) Kelly AFB, TX	Provides comprehensive IO support to the JFC and facilitates the integration of IO into military operations. Supports planning, coordination, and execution of DOD IO worldwide.
4th Psychological Operations Group (POG) (Airborne) Fort Bragg, NC	The only active Army PSYOP unit.
National Air Intelligence Center (NAIC) Wright-Patterson AFB, OH	Primary DOD producer of foreign aerospace intelligence. Assesses foreign capabilities; develops targeting and mission planning intelligence materials; and evaluates evolving technologies of potential adversaries.
Joint Warfare Analysis Center (JWAC) Dahlgren, VA	Primarily responsible for the integration and analysis of scientific and technical data related to warfare planning against infrastructure networks of selected countries of interest. Supports military operations and recommendations for deliberate and crisis planning. Products include high-leverage targeting options directed at enemy infrastructure (electric power, petroleum, oils and lubricants, lines of communications, and telecommunications). Also tasked with evaluating weapons' capabilities against critical components of selected targets, assessing the effects attacks on infrastructure networks have on the abilities of enemy fielded forces to conduct offensive or defensive operations, providing input from this analysis to intelligence organizations, and providing BDA indications for network and critical node failure analysis through the Joint Chiefs of Staff (JCS).
Information Operations Technology Center (IOTC) Fort Meade, MD	A joint DOD/intelligence community center of excellence tasked with developing and maintaining a computer/network technology-based toolbox of techniques and applications for the warfighter.
Joint COMSEC Monitoring Agency (JCMA) Fort Meade, MD	A field operating agency of the JCS. It was created in 1993 by a Memorandum of Agreement between the service operations deputies and directors of the joint staff and NSA. The JCMA is charged with conducting COMSEC monitoring (collection, analysis, and reporting) of DOD telecommunications and AIS and monitoring of related noncommunications signals.
Fleet Information Warfare Center (FIWC) Little Creek Amphibious Base, Norfolk, VA	Established as the fleet commander's authority for developing IW/command and control warfare (C2W) related tactics, procedures, and training, and for identifying requirements for IW/C2W research, development, test, and evaluation (RDT&E), acquisition, training and fleet staff augmentation. Also maintains a Navy Computer Incident Response Team.
Information Warfare Support Cell (IWSC/ P42) Fort Meade, MD	Provides information support, targeting, analysis, assessments, and intelligence gain/loss assessments. Also serves as the special technology office for NSA.

Organization and Location	Description
1st Information Operations Command (Land) (1IOC[L]) Fort Belvoir, VA	Formerly known as the land information warfare activity. Supports land component and Army commands to facilitate IO planning and execution. It enhances worldwide force protection by carrying out a proactive defense of Army information and information systems.
Defense Information Systems Agency (DISA) Washington, DC	DOD agency responsible for information technology and central management of major portions of the defense information infratstructure. Mission is to plan, engineer, develop, test, manage programs, acquire, implement, operate, and maintain information systems for C4I and mission support under all conditions of peace and war. Has defensive IO responsibilities.
Information Systems Security Office (ISSO) Fort Meade, MD	Provides information protection products and services for DOD and other government information systems. Provides technical vulnerabilities and threat assessments when tasked.
National Security Agency (NSA)/ Central Security Service (CSS) Fort Meade, MD	Responsible for the centralized coordination, direction, and performance of highly specialized technical functions in support of US Government activities to protect US communications and produce foreign intelligence information.
Naval Information Warfare Activity (NIWA) Washington, DC	The Navy's principal technical agent and interface to Service and national level agencies engaged in IW technologies. Is also the primary technical interface with FIWC for the transition of IW special technical capabilities for naval and Navy-supported joint operations. Conducts technical threat analysis and vulnerabilities assessment to develop requirements for evaluating new information technologies, competitive architectures, and advanced concepts for offensive and defensive IW systems.
Joint Spectrum Center (JSC) Severn River Naval Complex, Annapolis, MD	A DISA field activity and DOD center of excellence for electromagnetic spectrum management matters supporting the joint staff (J-6). Assists in managing joint restricted frequency list and resolving interference and jamming incidents.
Joint Communications Support Element (JCSE) MacDill AFB, FL	A deployable tactical communications unit under the operational control of the joint staff. Provides Chairman of the Joint Chiefs of Staff (CJCS)-directed contingency and crisis communications to meet operational and support needs of the JCS, Services, Unified Commands, Defense Agencies, and non-Defense agencies.

APPENDIX D. GLOSSARY
SECTION I. ACRONYMS AND ABBREVIATIONS

AIS . . . . . automated information systems

BDA . . . . . battle damage assessment

C2 . . . . . command and control
C2W . . . . . command and control warfare
C4 . . . . . command, control, communications, and computers
C4I . . . . . command, control, communications, computers, and intelligence
C4ISR . . . . . command, control, communications, computers, intelligence, surveillance and reconnaissance
CA . . . . . civil affairs
CAG . . . . . civil affairs group
CCIR . . . . . commander's critical information requirements
CE . . . . . command element
CI . . . . . counterintelligence
CJCS . . . . . Chairman of the Joint Chiefs of Staff
CJCSI . . . . . Chairman of the Joint Chiefs of Staff instruction
CJCSM . . . . . Chairman of the Joint Chiefs of Staff manual
CMO . . . . . civil-military operations
CNA . . . . . computer network attack
CND . . . . . computer network defense
CNE . . . . . computer network exploitation
CNO . . . . . computer network operations
COA . . . . . course of action
COG . . . . . centers of gravity
COMSEC . . . . . communications security

DCID . . Director of Center Intelligence Directive
DISA . . . . Defense Information Systems Agency
DOD . . . . . Department of Defense
DODD . . . . . Department of Defense directive
DODI . . . . . Department of Defense instruction

EA . . . . . electronic attack
EMW . . . . . Expeditionary Maneuver Warfare
EP . . . . . electronic protection
ES . . . . . electronic warfare support
EW . . . . . electronic warfare
EWCC . . . . . electronic warfare coordination cell
EWO . . . . . electronic warfare officer

FM . . . . . field manual (army)
FIWC . . . . . fleet information warfare center

G2 . . . . . intelligence officer (major subordinate commands and larger organizations
G3 . . . . . operations officer (major subordinate commands and larger organizations)

HUMINT . . . . . human intelligence

IA . . . . . information assurance
IAVA . . . . . Information Assurance Vulnerability Alerts
IMINT . . . . . imagery intelligence
INFOCON . . . . . information operations condition
INFOSEC . . . . . information security
IO . . . . . information operations
IOTC . . . . . Information Operations Technology Center
IPB . . . intelligence preparation of the battlespace
ISR . . . . . intelligence, surveillance, and reconnaissance
ISSO . . . . . information systems security officer
IW . . . . . information warfare
IW-D . . . . . defensive information warfare
IWSC . . . . . Information Warfare Support Center

J6 . . . . . command, control, communications, and computer systems directorate of a joint staff
JCEWS . . . . . joint commander's electronic warfare staff
JCMA . . . . . joint COMSEC monitoring activity
JCS . . . . . Joint Chiefs of Staff
JCSE . . . . joint communications support element
JFC . . . . . joint force commander
JIOC . . . . . Joint Information Operations Center
JP . . . . . joint publication
JPOTF . . joint psychological operations task force
JSC . . . . . Joint Spectrum Center
JTF . . . . . joint task force

JTF-CNO . . . . . Joint Task Force Computer Network Operations
JWAC . . . . . joint warfare analysis center

MAGTF . . . . . Marine air-ground task force
MARCERT . . . . . Marine Computer Emergency Response Team
MARFOR-INO . . . . . Marine Forces Information Network Operations
MCEN . . . . . .Marine Corps enterprise network
MCPP . . . . . .Marine Corps Planning Process
MCWP . . Marine Corps Warfighting Publication
MEF . . . . . Marine Expeditionary Force
MEU . . . . . Marine Expeditionary Unit
MITNOC. . . . . Marine Corps Information Technology and Network Operations Center

NAIC. . . . . National Air Intelligence Center
NCIS . . . . . Naval Criminal Investigative Service
NGO . . . . . .nongovernmental organization
NIWA . . . . . .naval information warfare activity

OPLAN . . . . . .operation plan
OPORD . . . . . .operation order
OPSEC . . . . . .operations security
OPT . . . . . operational planning team

PA. . . . . public affairs
PAO . . . . . .public affairs officer
POG . . . psychological operations group (Army)
PSYOP . . . . . psychological operations

RadBn . . . . . radio battalion
ROE . . . . . .rules of engagement

S2 . . intelligence officer (units and organizations below the major subordinate command level)
S3 . . . operations officer (units and organizations below the major subordinate command level)
SI. . . . . .special intelligence
SIGINT . . . . . .signals intelligence
SIO . . . . . .special information operations
STO. . . . . special technical operations

US . . . . . United States
USSTRATCOM . . . . . US Strategic Command

VMAQ . . . . . .Marine Tactical Electronic Warfare Squadron

1IOC(L) . . . . . 1st Information Operations Command (Land)

SECTION II. DEFINITIONS

civil affairs—Designated Active and Reserve component forces and units organized, trained, and equipped specifically to conduct civil affairs activities and to support civil-military operations. See also civil affairs activities; civil-military operations. Also called CA. (JP 1-02)

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

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

computer network defense—Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Also called CND. (JP 1-02).

computer network exploitation—Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. (DODI 3600.1)

computer network operations—Comprised of CNA, CND, and related CNE enabling operations. (DODI 3600.1)

counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (JP 1-02)

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

electronic warfare—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. (a.) electronic attack. That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: (1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming

and electromagnetic deception, and (2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). (b.) electronic protection. That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. (c.) electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 1-02)

information assurance—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. (JP 1-02)

operations security—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

physical security—(DOD, NATO) 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 1-02)

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

public affairs—Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA. (JP 1-02)

APPENDIX E
REFERENCES

Department of Defense Directive (DODD)

S-3600.1	Information Operations

Department of Defense Instruction (DODI)

5200.40	DOD Technology Security Certification and Accreditation Process (DITSCAP)

Chairman of the Joint Chiefs of Staff Manual (CJCSM)

3122.03	Joint Operational Planning and Execution System Volume II, Planning Formats and Guidance

Chairman of the Joint Chiefs of Staff Instruction (CJCSI)

6510-01C	Information Assurance and Computer Network Defense

Joint Publications (JPs)

1-02	Department of Defense Dictionary of Military and Associated Terms
3-13	Joint Doctrine for Information Operations
3-54	Operations Security
3-58	Joint Doctrine for Military Deception

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-0.1	Componency
2	Intelligence

Marine Corps Warfighting Publications (MCWPs)

2-1	Intelligence Operations
2-14	Counterintelligence
3-16	Fire Support Coordination in the Ground Combat Element
3-33.1	Marine Air-Ground Task Force Civil-Military Operations
3-33.3	Marine Corps Public Affairs
3-40.2	Information Management
3-40.3	Communications and Information Systems
3-40.6	Psychological Operations

Army Field Manual (FM)

34-130

Director of Central Intelligence Directive (DCID)

6/3
7/3

Miscellaneous

Computer Security Act of 1987
Public Law 100-235