MCWP 3-32
(Formerly MCWP 3-40.4)

Marine Air-Ground Task Force Information Operations

US Marine Corps

PCN 143 000140 00

CD&I (C 116)

2 May 2016

ERRATUM

to

MCWP 3-40.4

MARINE AIR-GROUND TASK FORCE INFORMATION OPERATIONS

1. Change all instances of MCWP 3-40.4, *Marine Air-Ground Task Force Information Operations*, to MCWP 3-32, *Marine Air-Ground Task Force Information Operations.*

2. File this transmittal sheet in the front of this publication.

PCN 143 000140 80

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes through the Universal Need Statement (UNS) process. The UNS submission process is delineated in Marine Corps Order 3900.15_, *Marine Corps Expeditionary Force Development System*, which can be obtained from the on-line Marine Corps Publications Electronic Library:

http://www.marines.mil/News/Publications/ELECTRONICLIBRARY.aspx.

The UNS recommendation 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
  - Addition/deletion of text
  - Proposed new text

Additional copies: If this publication is not an electronic only distribution, a printed copy 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 United States Marine Corps Doctrine web page:

https://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, D.C. 20380-1775

1 July 2013

FOREWORD

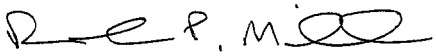
Marine Corps Warfighting Publication (MCWP) 3-40.4, *Marine Air-Ground Task Force Information Operations*, operationalizes the *Marine Corps Operating Concept for Information Operations*. This publication contains doctrine for employment of the various information-related capabilities integrated as information operations in support of the Marine air-ground task force (MAGTF).

The purpose of this publication is to provide MAGTF commanders and their staffs guidance in planning, preparing, executing, and assessing information operations in support of the MAGTF's operational objectives. It gives Marines a warfighter's orientation to information operations, providing a basis to understand the relevance of information operations and a framework to implement information operations.

This publication is intended for Marines assigned to a MAGTF that are responsible for information operations planning.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS



RICHARD P. MILLS
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development and Integration

Publication Control Number: 143 000140 00

This Page Intentionally Left Blank

MARINE AIR-GROUND TASK FORCE INFORMATION OPERATIONS

TABLE OF CONTENTS

Chapter 4. Information Operations Intelligence Integration

Appendices

Glossary

References and Related Publications

This Page Intentionally Left Blank

CHAPTER 1
FUNDAMENTALS

As defined in Marine Corps Reference Publication (MCRP) 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*, information operations (IO) are the integration, coordination, and synchronization of all actions taken in the information environment to affect a relevant decisionmaker in order to create an operational advantage for the commander. The Marine air-ground task force (MAGTF) executes IO as an inherent element of all operations to enable and enhance the overall ability to conduct successful military actions. In order to apply information operations across a range of military operations, the MAGTF commander integrates his military actions, forces, and capabilities throughout the operational environments (air, land, maritime, and space domains and information environment). These efforts can create and/or sustain desired and measurable effects on the adversary's leaders, forces (regular or irregular), information, and information systems and other audiences; while protecting and defending the MAGTF commander's forces, information, and information systems.

As with other elements of combat power, there is no universal formula for the application of information operations; therefore, information operations should be viewed as an element of combat power, focusing on when and where it best supports MAGTF operations. The factors of mission, enemy, terrain and weather, troops and support available—time available and, when required, civilian considerations are the major determinants.

Information operations are primarily concerned with affecting decisions and decisionmaking processes while at the same time defending friendly decisionmaking processes in order to achieve information superiority. Information operations affect and defend decisionmaking based on six fundamental assumptions:

- Decisionmakers generally value the quality of information they receive.
- The influences of geography, language, culture, religion, organization, experience, and personality of the decisionmaker impact the relative value placed upon the information received.
- Decisions are made based on the information available at the time.
- It is possible, with finite resources, to understand the relevant aspects of the information environment to include the processes decisionmakers use to make decisions.
- It is possible to affect the information environment in which specific decisionmakers act through psychological, electronic, or physical means.
- It is possible to measure the effectiveness of IO actions in relation to an operational objective.

Although each of these assumptions is an important enabling factor for information operations they may not all be true for every operation. For any specific operation where one or more of these assumptions are not met, the risk assessment provided to the commander would be adjusted accordingly.

Marines deploy as unique, task-organized MAGTFs and their ability to task-organize and integrate the necessary combat power to achieve the objective is part of their expeditionary mindset. Therefore, the integration of information operations into the Marine Corps Planning Process (MCPP) is critical.

Legal Considerations

Information operations may involve complex legal and policy issues requiring careful review. Similar to operations in the physical environment, MAGTF activities in the information environment are bounded by policy, societal values, and a fundamental respect for human dignity. Marines, whether operating physically from bases or locations overseas or from within the boundaries of the United States, are required by law and policy to act in accordance with US law and other standards of conduct (e.g., law of war [often called the law of armed conflict], rules of engagement). Because of the potential numerous legal issues associated with information operations, it is critical to obtain a legal analysis of the proposed operation within the context of the applicable law, ideally through the judge advocate's participation within an IO planning cell. This individual should be consulted early and often to ensure compliance and eliminate potential delay. If, based on lack of capacity, a judge advocate cannot be a permanent member, an open and continuous dialogue must be established with the staff judge advocate (SJA).

Information Environment

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (Joint Publication [JP] 1-02, *Department of Defense Dictionary of Military and Associated Terms*) Therefore, a solid understanding of the information environment must be achieved before any planning can begin. Refinement of the command's understanding of the information environment continues throughout the planning process and the execution of operations. The information environment consists of three interrelated dimensions: cognitive, informational, and physical. Table 1-1 represents a typical view of the three interrelated dimensions and some of their characteristics.

Table 1-1. Dimensions of the Information Environment.

Cognitive Dimension	Exists in the minds of human beings. Consists of individual and collective consciousness. Exists where information is used to shape perceptions and make decisions. Significant characteristics include values, beliefs, perceptions, awareness, and decisionmaking.
Informational Dimension	Created by the interaction of the physical and cognitive dimensions. Exists where information is collected, processed and disseminated. Significant characteristics are information content and flow.
Physical Dimension	Consist of the tangible, real world. Exists where information environment overlaps with the physical world. Consists of individuals, organizations, information systems, and the physical networks that connect them. Significant characteristics include terrain, weather, civilian information infrastructure, media, populace, and third party organizations.

Cognitive Dimension

The cognitive dimension consists of the beliefs of a person or persons whose decisions can impact the commander's end state and is the hardest dimension to assess. The key to understanding this dimension is understanding that decisions are made based on culture, life experiences, relationships, outside events, ideology, and the influences of those inside and outside a decisionmaker's group. Added to these variables are the perceptions that are built on information collected on current events and the plans and beliefs of others. Ultimately, the commander must determine how a targeted decisionmaker will act on his beliefs and perceptions and how that action will impact the commander's end state.

Informational Dimension

The informational dimension consists of the content of information and the way it flows to and from a decisionmaker to form a message. The content of the message is the idea or thought that is conveyed to key audiences. The message must flow so its intended audience can actually hear, read, or see it.

Physical Dimension

The physical dimension consists of both key individuals and human networks and a technical and physical infrastructure that supports the information flow to its intended audience:

- Key individuals are those that provide access to audiences of interest, have the ability to influence target audiences, or may be the audience of interest themselves.
- Human networks are groups that support the process and dissemination of information to an audience. They can also shape the beliefs of others based on their own ideology and goals.
- Technical infrastructure is what is needed to produce, process, receive, send, and store information so that the decisionmaker can interact with others and make decisions.
- The physical infrastructure supports the flow of information and is what houses the technical infrastructure, as well as key individuals and human networks.

Use of Information

Part of understanding a target audience's information environment is to understand how the target audience leverages information within that environment. When assessing a target audience's use of information, it is important not to mirror the discussion with US abilities. Depending on the sophistication of the audience, they may or may not have the same capabilities as the United States. An IO planner must fully validate any assumptions about a target audience's capabilities to leverage information prior to the end of the planning phase. The IO planner's analysis of an adversary target audience's methods of leveraging information must address the target audience's ability to protect, collect, and project information:

- How will the target audience leverage information within their operational environment in order to achieve their goals?
- How will the target audience protect information that is deemed critical (information required to make decisions without being interrupted)?
- How will the target audience collect—either overtly or covertly—information on its adversaries so they can make decisions that best support their goals?
- How will the target audience project information to others in order to persuade others to support their goals?

Information Superiority

Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02) Obtaining the operational advantage described within the definition of information superiority is the overarching focus of information operations. Just as each mission's end state is different, so is information superiority. For example, during combat operations, information superiority can gain surprise over the adversary or prevent the adversary from employing its reserve forces. During counterinsurgency operations, information superiority can gain populace support for friendly operations or prevent adversary freedom of information flow. In each case, information superiority is defined specifically for the mission in terms of what advantage is sought for the MAGTF.

Gaining information superiority over the adversary should always be the main effort of information operations. To achieve information superiority, the MAGTF uses information to actively attack the adversary and to shape the information environment to the MAGTF's advantage. This duality of operations is analogous to fire and maneuver where fires equate to attacking the adversary's ability to use information and maneuver equate to actions that seize and retain information nodes for the purpose of gaining a positional advantage. To be effective, information operations must balance activities that shape the information environment with those that attack the adversary. Through a combination of both, the MAGTF seeks information superiority over its opponent.

The MAGTF will rarely achieve absolute and universal information superiority. The actions of opposing forces, as well as the information content and flow in the operational area, are not static. Therefore, information superiority is a localized and transitory condition over the adversary. The MAGTF seeks information superiority at certain times and places, usually at or before the decisive point of the operation.

Information-Related Capabilities

Military operations are not planned for the purpose of employing any particular capability. Mission requirements (such as campaign objectives, the operational environment, and adversary and friendly forces) dictate what capabilities a commander uses and how they are employed. Information operations are no different.

Although often described as a discrete set of capabilities, information operations are really much more. The capabilities used for information operations should be selected based on mission requirements. Such a capability is, according to JP 1-02, a capability, function, or activity that uses data, information, or electromagnetic spectrum to produce lethal or nonlethal effects in the physical or informational dimensions with an expressed intent to cause deliberate effects within the cognitive dimension of the information environment.

Some information-related capabilities (IRCs), such as electronic warfare (EW), military information support operations (MISO), combat camera (COMCAM), and cyberspace operations, require trained specialists and equipment. However, each element of a MAGTF must be able to employ other capabilities, such as operations security (OPSEC), military deception (MILDEC), key leader engagements, and a rewards program to support its operations. Refer to chapter 3 for a discussion on capabilities relevant to information operations.

Information Operations Effects

Commanders use IRCs to create or produce effects that contribute to the achievement of military objectives. Numerous common terms, such

as the following, are used but have unique meanings when describing IO effects:

- *Destroy*. Destroy is to damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.
- *Disrupt*. Disrupt is to break or interrupt the flow of information.
- *Degrade*. Degrade is to reduce the effectiveness or efficiency of an adversary's command and control (C2) or communications systems and information collection efforts or means. Information operations can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of an adversary's decisions and actions.
- *Deny*. Deny is to prevent the adversary from accessing and using critical information, systems, and services.
- *Deceive*. Deceive is to cause a person to believe what is not true. Military deception seeks to mislead an adversary's decision-makers by manipulating their perception of reality.
- *Exploit*. Exploit is to gain access to an adversary's C2 systems to collect information or to plant false or misleading information.
- *Influence*. Influence is to cause others to behave in a manner favorable to US forces.
- *Isolate*. Isolate is to seal off both physically and psychologically an adversary from its sources of support, to deny an adversary freedom of movement, and prevent an adversary unit from having contact with other adversary forces.
- *Protect*. Protect is to take action to guard against espionage or capture of sensitive equipment and information.
- *Restore*. Restore is to bring information and information systems back to their original state.
- *Respond*. Respond is to react quickly to an adversary's IO attack or intrusion.

Note: The preceding effects terms can have different interpretations. The above list is accepted in joint doctrine for information operations. They may not align with Marine Corps terms for the effects of fires (lethal). It is always best to define how the term is being applied with respect to IO tasks.

This Page Intentionally Left Blank

CHAPTER 2
INTEGRATION AND PLANNING

The primary focus of MAGTF IO activities will be at the operational and tactical levels of war. The Marine Corps organizes, trains, equips, 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. Information operations are conducted across the range of military operations. Information operations can make significant contributions to all levels of warfare. Information operations should not be relegated to just one type of military operation. Information operations are conducted during all phases of military operations. Information operations are planned, prepared, executed, and assessed during all phases of an operation in support of the MAGTF's mission.

Since MAGTFs may fight as a part of a larger joint force, their IO efforts will support and be coordinated with the campaign plans of the combatant commander, joint force, and adjacent commands. The joint force commander 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 will develop their own IO plans in support of their respective objectives. These IO plans are typically at the operational level. The MAGTF will develop an IO plan that will support MAGTF mission requirements while integrating the joint force commander's IO plan. The major subordinate commands must develop supporting IO plans that are appropriate for their level of command.

Staff Responsibilities

Although information operations are not limited to the IRCs, they do encompass all actions taken to affect the decisionmaking within the information environment; therefore, IO planning requires a whole-of-staff approach in order to be effective. Those staff sections involved in IO planning include, but are not limited to, the operations section, intelligence section, communications sections, special staff, and IO cell.

While the commander has overall responsibility to decide and design how and who he wants to influence, his IO cell chief—residing within the G-3—has responsibility to plan, prepare, execute, and assess information operations in support of operations. All staff sections have a role to play in information operations. To relegate information operations to just one subsection of the G-3 severely limits the command's IO program and its effectiveness. Information operations that are not integrated with other staff actions often lead to instances where actions interfere with each other and are counterproductive to achieving the commander's desired effects. At best, nonintegrated information operations reduce the effectiveness of the action and, at worst, confuse the target audience leading to undesired effects.

Operations Section

The commander is responsible for implementing plans that incorporate information operations into operations, but the operations section (G-3/S-3) is responsible for executing the plans. The future operations (FOps) section is responsible for overseeing the planning and coordination of the IO effort. The MAGTF IO officer, within G-3/S-3 FOps, is responsible for the following:

- Integrating and coordinating IO efforts.
- Responding directly to the commander via the G-3/S-3 for MAGTF information operations.
- Ensuring that the IO cell is incorporated into and provides input to the operational planning

team (OPT) during planning to ensure coordinated operations.
- Preparing the IO appendix to the operation order (OPORD).
- Directing personnel within the MAGTF IO cell as well as augmentees from external agencies who are assigned to the IO cell.
- Ensuring that all information operations are coordinated within the MAGTF staff, higher headquarters, and external agencies.
- Coordinating and collaborating with the intelligence staff section (G-2/S-2).

The electronic warfare officer (EWO) will integrate EW operations through the EW coordination center or the IO cell when it is established.

The fire support coordinator, supporting arms coordinator, target information officer, and target intelligence officer will oversee the formation of the target list and the engagement of those targets, to include accepted targets nominated by the IO cell.

Public affairs officers (PAOs) will identify key public or target audiences with interest and impact in the area of operations, to include foreign and domestic audiences and local, regional, and international media. Public affairs and IO planners must plan, coordinate and deconflict activities, release of public information, and media analysis/assessment to achieve maximum effect, consistent with the Department of Defense (DOD) principles of information, policies, and public affairs (PA) guidance.

The COMCAM planner ensures that priorities are established for the provision of visual documentation for operational and combat support.

The civil affairs (CA) officer identifies key civil-military operations (CMO) targets and coordinates with the targeting cell. He provides the local populace news and information about CMO activities and support, which aids in neutralizing misinformation and hostile propaganda directed against civil authorities.

The current operations officer will assist the IO officer in the supervision and coordination of IO activities that support or are integrated into ongoing operations. The current operations officer supervises battle captains/watch officers and communicates with subordinate commanders to identify and monitor IO events within the MAGTF's area of operations. Additionally, the current operations officer must be prepared to execute IO battle drills if required.

The FOps officer will work closely with the IO officer to monitor current operations and ensure that planned MAGTF operations are conducted in order to achieve objectives across the operational environment. The FOps officer must be particularly mindful to ensure that operations in the physical dimension support the commander's objectives in the informational and cognitive dimensions.

Intelligence Section

Intelligence is critical to the planning, execution, and assessment of information operations and must provide support across a range of military operations at all levels of war. The G-2/S-2 is the central point of contact for all intelligence support to information operations 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 appendix A.

Communications Section

The communications section (G-6/S-6) oversees the communications security (COMSEC) program, supports the installation and maintenance of information systems, assists the EWO in deconflicting EW jamming operations in order to avoid electronic fratricide, and coordinates active OPSEC measures and facilitation of specialized communications in support of IRCs and information operations.

Special Staff

In support of the MAGTF mission, public affairs assists the MAGTF IO officer in keeping local populations informed by putting MAGTF actions into context, countering propaganda and misinformation, and by communicating proposed MAGTF actions in order to deter the adversary's actions. These efforts build support for military operations, help the local population develop informed perceptions about MAGTF activities, undermine adversarial propaganda, and shape the adversary's planning.

Chaplains, though not a traditional IRC, have a very important role to play in information operations. Recent operations in both Iraq and Afghanistan have seen the adversary use religion to bolster and justify recruiting and terrorist activities. Chaplains participating in key leader engagements can assist in co-opting religious leaders and degrading the adversary's use of religion.

The civil affairs officers from the G-9/S-9 section assist the MAGTF IO officer in integrating planned CMO into the information operations to ensure that information operations and CA are creating the most favorable effects for the MAGTF commander and are not at odds with the effects created in specific areas of the operational environment.

The SJA supports the MAGTF IO officer by ensuring all phases of the operation, to include any branches and sequels, are conducted in compliance with the applicable laws. In so doing, the SJA plays a critical role in the development and refinement of a proposed course of action (COA). The SJA should be involved early in IO planning in order to avoid delays in the execution of IO-related actions.

Information Operations Cell

The IO cell is a task-organized group that will be established within a MAGTF and/or higher headquarters to integrate a variety of separate disciplines and functions pertaining to information operations 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. Information operations 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.

The IO cell is composed of intelligence personnel, augmentees supporting IO activities, and representatives from staff elements and subject matter experts (SMEs) from appropriate warfighting functions. The size and structure of the cell are tailored to meet the mission and the commander's intent.

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

Integrated Information Operations Planning and the Marine Corps Planning Process

The commander and his planners must ensure that information operations 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 MAGTF's concept of operations. Military deception, MISO, and cyberspace operations require more time to plan due to the authorities that are required to execute these activities and the time required to establish and prepare observables for these activities.

Marines use the MCPP and the targeting process (D3A [decide, detect, deliver, assess]) in the

development of the IO concept of support and IO plans. Two notable requirements in IO planning are as follows:

- A longer lead time is required to plan certain information operations (i.e., MILDEC, MISO, and cyberspace operations).
- The impact and threat of hostile information from outside the operational area due to the ease of information flow through information networks and the media, which creates operating boundaries in the information environment that are larger than the area of operations and are porous to outside influences.

During the planning process, the IO officer must be prepared to quickly articulate IO objectives and provide detailed information on how the integration of discrete IRCs will support the commander's desired end state.

The MCPP establishes procedures for analyzing a mission, developing and wargaming COAs against the adversary, comparing friendly COAs against the commander's criteria and each other, selecting a COA, and preparing an OPORD execution. Information operations planning is aligned with the MCPP steps and ensures that IO actions are coordinated with all six warfighting functions and the operations of higher, adjacent, and subordinate commands. See Marine Corps Warfighting Publication (MCWP) 5-1, *Marine Corps Planning Process*, for detailed information.

Problem Framing

The purpose of problem framing is to gain an enhanced understanding of the environment and the nature of the problem. This understanding allows a commander to visualize the operation and describe his conceptual approach, providing context for the examination of what the command must accomplish, when and where it must be done, and most importantly, why the operation is being conducted. Since no amount of subsequent planning can solve a problem insufficiently understood, problem framing is critical.

The higher headquarters order is analyzed to extract IO planning guidance, such as limitations and planning factors. This guidance establishes the boundaries for IO planning, identifies target limitations based on policy and rules of engagement, 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 problem framing, intelligence preparation of the battlespace (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 adversary and the information environment. Key actors must be identified early in the planning process. A key actor is a person or persons whose decisions will have an impact, either positively or negatively, on the commander's end state. As the planning process matures, these key actors may become the command's target audience, at which time, effort and resources are applied in order to effect their decisions. Intelligence preparation of the battlespace products relevant to further IO planning are developed or requested. Adversary centers of gravity (COGs) are determined, while potential risks and friendly vulnerabilities are also identified. Information gaps must be determined and requests submitted to resolve the uncertainties necessary for further planning. During the planning process, IO planners conduct an analysis that links national, combatant command, or joint strategic objectives to the MAGTF's operational and tactical tasks. By linking operational level objectives and tasks to strategic objectives, the IO planner will ensure that MAGTF activities are in concert with higher headquarters' desired end state.

An initial IO concept for support can be developed during problem framing. Friendly IO assets and capabilities, either organic or supporting the MAGTF, as well as additional IO force structure requirements, are identified. As problem framing is conducted, resource or capability shortfalls are noted. The IO cell identifies critical shortfalls and

requests support from higher headquarters or external agencies to achieve projected, desired results. 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 IO concept of support and should be developed.

The IO cell must fully participate in MAGTF planning activities and coordinate its planning efforts with those of the MAGTF FOps section. An ad hoc organization known as the OPT (the IO cell should have a representative in the OPT) is usually formed by the FOps section. The OPT will be conducting problem framing. The results of each group's OPT and IO cell analyses should be combined. Friendly vulnerabilities can be incorporated into force protection planning, while the adversary's critical vulnerabilities determined through the OPT's COG 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 operations.

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

At the end of problem framing, IO personnel should have developed the following:

- Staff estimate for information operations.
- A combined information overlay and a template of adversary operations in the information environment.
- An understanding of which decisionmakers should be targeted.
- IO essential tasks.
- Shortfalls in IRCs.
- IO limitations.
- IO critical information requirements.

Appendix B provides several examples of IO planning products.

Essential Tasks for Information Operations

Rarely will the MAGTF conduct information operations by itself. There will always be higher headquarters guidance and tasks. While some tasks may have been specifically assigned by the higher headquarters, others may be implied, meaning they are necessary to accomplish specified tasks or the overall mission. Implied tasks require resources and may not be administrative in nature. From the specified and implied tasks, IO personnel identify tasks that the command must accomplish to successfully affect adversary and friendly use of information. These become the unit's essential tasks for information operations. Essential tasks for information operations should be limited to no more than five; any more than that will overburden the subordinate element with developing tasks in support of essential IO tasks or may create an information operation that is too complex to execute.

A rule of thumb for validating an essential task is to ask: If the MAGTF accomplishes all other tasks marginally and does this one well, will it accomplish the mission? If the answer is no, then the task is not essential. If more than five essential tasks are identified, then IO personnel should question the validity of each essential task or the nature of the requirements levied on the MAGTF by higher headquarters.

Shortfalls in Information Operations Capabilities

Information operations personnel should determine if the MAGTF has the assets to perform the assigned tasks. This is done by identifying any and all organic and supporting IO-capable assets. Organic assets are resident in assigned or attached forces. Supporting assets are available to the MAGTF from a higher headquarters or US Government agency. Available assets are then compared with the IO mission requirements (specified and implied tasks) in order to identify capability shortfalls and any additional assets that are required. To ensure use of these assets, IO personnel must start coordination early.

Information operations planners face a challenge in expressing IO capabilities to the commander and staff. A simple list of IO-capable assets or units—such as, three ground-based jammers, three tactical MISO teams, or two COMCAM teams—does not help the commander visualize the command's capabilities in the information environment. In developing its product, IO personnel should consider three basic questions:

- What IO effects can be created or produced using the command's organic assets?
- What IO effects can be created or produced using supporting assets from the higher headquarters?
- What IO effects cannot be created or produced with available assets?

Restraints and Constraints for Information Operations

Restraints are the things that you cannot do and constraints are the things that you must do that do not qualify as specified tasks, but need to be identified and carried forward into COA development and subsequent planning as they can affect how operations will be conducted.

Like most other operations, information operations are restrained by rules of engagement; US national policy; international politics; and other legal, moral, cultural, and operational factors. Additionally, IO personnel should consider that IRCs have restraints of their own; in particular, MILDEC, MISO, cyberspace operations, and electronic warfare. Common restraints include approval authorities for deception operations, MISO products, MISO themes to avoid, allied forces' national policies and capabilities, restricted targets and frequencies, and PA guidance. To enhance understanding, limitations for information operations can be organized in terms of information content and flow.

Information content is the substance, value, or meaning of the information, normally comprised within the words and images; includes the intended action or inaction the information was designed to elicit. Examples include the following:

- Avoid themes that favor any ethnic group.
- Receive MISO product approval from the combatant commander.
- Receive deception approval from joint task force (JTF) commander.
- Stress themes that highlight the importance of reconciliation.

Information flow describes how information is transferred or exchanged between a transmitter/source and a receiver and includes the means, mediums, and paths utilized in the exchange. Examples include the following:

- No cross-boundary electronic attack.
- US MISO products cannot be disseminated by allied forces.
- PA posture for the operation is passive.
- Religious structures are identified on the restricted target list.
- COMCAM priorities.

Critical Information Requirements for Information Operations

Only the commander decides what information is critical, but the staff may propose CCIRs to the commander. The CCIRs are continually reviewed and updated or deleted as required. Initially, CCIRs may reflect the nature of planning and identify intelligence or information requirements to assist with the planning and decision process. As the planning moves forward and execution looms, CCIRs will normally change to reflect key information/intelligence requirements tied to decision points or needed for execution.

Course of Action Development

During COA development, planners use the mission statement, commander's intent, and commander's planning guidance to develop COAs.

Course of action development provides options for how the mission and commander's intent might be accomplished while continuing to refine the understanding of the problem. The IO planner's goal is to develop a concept of support that will generate effects that create information superiority over the adversary at the proper time and place. An IO concept of support should be 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 that is started during problem framing will continue during COA development. The IPB products that are requested and developed will be reviewed for applicability with the commander's planning guidance. As necessary, IO-related IPB products will be modified and updated. As new information is received, CCIRs may be revised and additional requirements submitted.

Information operations cell planning efforts will continue to be closely linked with those of the OPT. The IO planner can assist the OPT by graphically displaying the significant characteristics of the information environment, allowing the OPT to see the capabilities of both friendly and adversary forces. See JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, for a detailed discussion on the combined information overlay. In coordination with the red cell and the G-2, the IO cell will conduct nodal analysis to assess relative IRCs and provide the OPT with an understanding of the strengths and weaknesses of both friendly and adversary forces. The IO cell will conduct an assessment of friendly vulnerabilities to adversary information actions. The IO cell will also continue to refine its analysis of the adversary COG to determine the critical adversary vulnerabilities most susceptible to information operations. The refined COG and critical vulnerabilities are used in the development of the initial COAs.

The IO cell will closely follow the development of the OPT's 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 will execute the IO tasks (IO assets capabilities)?
- When will IO tasks be executed?
- Where will the IO tasks occur?
- Why is each IO task required (intended effect)?
- How will the MAGTF employ IRCs and other organic capabilities to accomplish the tasks?
- How is the IO concept nested with the higher headquarter's IO plan and scheme of manuever?

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 to include objectives and purposes for essential IO tasks, target nominations, and an assessment plan to measure the effectivness of the tasks.
- 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 information operations with additional asset requirements or required support from higher headquarters.

Course of Action War Game

The COA war game examines and refines the broad option(s) in light of adversary capabilities and potential actions/reactions as well as the characteristics peculiar to the operational

environment. Each friendly COA is wargamed against selected adversary COAs. Course of action wargaming assists the planners in identifying strengths and weaknesses, associated risks, and asset shortfalls for each friendly COA. The IO cell's 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, while also fully participating in the COA war game. The IO actions are integrated into the COA war game in an interactive process to determine the impact on both friendly and adversary capabilities. The IO cell should observe and record the advantages and disadvantages of each COA and the capability of information operations to support each COA. For future planning, it should also identify possible branches and potential sequels based on the IO concept.

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 input to IPB products.
- Refined staff estimate for information operations.
- Refined input to CCIRs.
- Task organization and asset shortfalls for IO resources.
- Information operations 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, against each other, and then selects the COA that will best accomplish the mission. As appropriate, the IO cell will provide additional comparison criteria directly relevant to information operations 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 commander is apprised of the effects that have been created by operations in the information environment. The IO cell is also responsible for ensuring that the impact and anticipated effect of IO actions upon the adversary targets 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, 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 information operations 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. Specifically, Appendix 3 (Information Operations) to Annex C (Operations) describes the information operation as a whole and how information operations will gain information superiority in support of the scheme of maneuver. See appendix C for a sample format of an OPORD. The IO cell must be careful to not let the requirement to develop and explain IRCs and contributions to the operation overwhelm the primary purposes of the IO appendix, which are to—

- Provide operational details on information operations.
- Focus element and unit tasks on creating specific effects in the information environment.
- Provide the information needed to assess information operations.

Because information operations are multidisciplined, it is found in various portions of the MAGTF OPORD. The disciplines of IO are included as tabs to Appendix 3 (Information Operations), Annex C (Operations) to the

OPORD and in the OPORD annexes for communication systems, public affairs, CMO, information management, and special technical operations (STO).

During orders reconciliation and crosswalk, the information operations cell may be called upon to review the IO sections of the orders, identify gaps in planning or discrepancies, provide corrective action, and finalize IPB products. If fragmentary orders are issued, then the IO cell will ensure that appropriate instructions are given to IO-capable units.

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 that there is a coherent shift from planning to execution and may involve a wide range of briefs, drills or rehearsals (subject to the variables of echelon of command), mission complexity, and, most importantly, time.

The IO cell monitors 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. 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.

Successful information operations give subordinates maximum latitude for initiative, and postures the unit for follow-on missions. Likewise, with a little foresight, IO personnel can use one information operation to jump start another. Occasionally, a tactical level information operation may be the perfect jump start for an operational level information operations and so on.

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 that are consistent with evolving operations. The MAGTF IO cell is useful in providing IO support to the steps of the MCPP and can help the MAGTF develop the following essential building blocks:

- Stated objectives (based on desired operational effect).
- IO synchronization matrix that links mutually supporting IO actions.
- Integrated target list.

These building blocks help sustain ongoing information operations. Sustained information operations are supported by the MAGTF intelligence cycle, battle damage assesment (BDA) cycle, targeting cycle, and the MAGTF operations battle rhythm. These processes allow the MAGTF to analyze the information intelligence cycle, assess the functional capability (or destruction) of the adversary BDA cycle, re-engage as necessary to maintain constant pressure on the adversary's targeting cycle, and modify and issue changes to ongoing plans. It is the integration of these cycles that determines the daily IO battle rhythm.

This Page Intentionally Left Blank

CHAPTER 3
KEY INFORMATION-RELATED CAPABILITIES

Information operations are multidisciplined and include a variety of elements that 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 operations that ensures successful employment of information operations in support of the MAGTF. Integration of information operations is an essential part of MAGTF operations in expeditionary and joint environments. Information operations can mitigate the effects of a crisis and can help prevent or resolve conflict.

When deterrence fails, information operations help Marines win in war by providing essential protection and enhancing the effective use of force. Information operations enhance the operational capability of the MAGTF through employment of a wide range of organic and external capabilities.

Military Deception

The purpose of MILDEC is to cause adversaries to form inaccurate impressions about friendly force capabilities or intentions by feeding information through their intelligence collection or information assets. Military deception targets the adversary decisionmaker's intelligence collection, analysis, and dissemination systems and requires a thorough knowledge of adversaries and their decisionmaking processes.

Military deception operations are actions executed to deliberately mislead the adversary's military decisionmakers as to friendly military capabilities, intentions, and operations; thereby, causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission.

Military deception operations depend on an integrated effort by all warfighting functions to create a credible 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 MILDEC 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 MILDEC operations. For more information on MILDEC, see JP 3-13.4, *Military Deception*, or the classified MCRP 3-40.4A, *Multi-Service Tactics, Techniques, and Procedures for Military Deception (MILDEC) Operations*.

Types of Deception Operations

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

A feint is a limited objective attack that involves contact with the adversary. 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 vary in size from a raid to a supporting attack. A feint may occur before, during, or after the main attack and may be independent of the main effort. Feints may be employed to cause the adversary to react in one of three predicable ways: employ his reserves improperly, shift his supporting fires, or reveal his defensive fires.

A demonstration is an attack or show of force on a front where a decision is not sought and made with the aim of deceiving the adversary. A demonstration differs from a feint in that no contact with the adversary is intended.

A ruse is a trick of war that places false information in the adversary'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 inconsistencies and may present the adversary 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 adversary's visual observation. Displays are simulations, disguises, or portrayals that project to the adversary 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 MILDEC 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 adversary 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 the adversary's 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

Operations security and deception have much in common. Both require the management of indicators. Operations security is used to deny information or to hide what is real and 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 or to show what is not real and seeks to create or increase the likely detection of certain indicators that the adversary can observe and that will cause an adversary to derive an incorrect conclusion.

Special Considerations for Deception Planning

When planning for deception operations, the staff must consider classification requirements as well as any possible unintended effects that may be a result of the operation:

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

- *Unintended Effects*. Third parties, such as neutral or friendly forces not aware of the deception, may receive and act upon deception information that is intended for the adversary. Deception planners should minimize the risk to other parties.

Staff 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 (Information Operations) of Annex C (Operations) of the OPORD is the deception tab. This tab implements the recommended COA for deception. The deception tab details the specific tasks to be performed and specifies coordinating instructions for the control and management of deception missions.

Electronic Warfare

Electronic warfare is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the adversary. (JP 1-02) Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support. Electronic warfare denies the opponent an advantage in the electromagnetic spectrum and ensures friendly unimpeded access to the electromagnetic spectrum portion of the information environment. Electronic warfare can be applied from air, sea, land, and space by manned and unmanned systems, and it is employed to support military operations involving various levels of detection, denial, deception, disruption, degradation, protection, and destruction. Contributing to the success of information operations, electronic warfare uses offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the electromagnetic spectrum while protecting friendly freedom of action in that spectrum. For more information on electronic warfare see JP 3-13.1, *Electronic Warfare*, or MCWP 3-40.5, *Electronic Warfare*.

Electronic Attack

Electronic attack is a 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. (JP 1-02) Electronic attack includes the following:

- Actions taken to prevent or reduce an adversary's effective use of the electromagnetic spectrum, such as jamming and the use of antiradiation weapons.
- Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism such as lasers, radio frequency weapons, and particle beams.

Electronic Protection

Electronic protection is a division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 1-02)

Electronic Warfare Support

Electronic warfare support is a division of electronic warfare involving actions tasked by, or under the 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. (JP 1-02)

Electronic warfare support provides information required for decisions involving EW operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence.

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), electronic warfare, and special intelligence communications support to the MAGTF. The role and structure of the RadBn continue to evolve with the evolution of communications technology.

A VMAQ provides EW support to the MAGTF and other designated forces. The VMAQ conducts tactical jamming to prevent, delay, or disrupt the adversary's ability to use early warning, acquisition, fire or missile control, counterbattery, and battlefield surveillance radars. Tactical jamming also denies and/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 [Marine Aircraft Group-14], 2d MAW [2d Marine Aircraft Wing]. Each squadron has five EA-6B Prowler aircraft.

Staff Responsibilities

Electronic warfare is the responsibility of the G-3/S-3. An EWO is normally appointed to be responsible for planning, coordinating, and tasking EW operations and activities. The EWO coordinates with the G-2/S-2 to establish priorities between EW and SIGINT missions. The EWO also coordinates with the G-6/S-6 to facilitate maximum use of the electromagnetic spectrum through electronic protection and to minimize electromagnetic interference.

Electronic Warfare Coordination Cell

The electronic warfare coordination cell (EWCC) is a dedicated EW planning cell that may be established to coordinate EW activities. The MAGTF commander will normally plan, synchronize, coordinate, and deconflict EW operations through the EWCC, which facilitates coordination of EW operations with other fires, communications systems, and information systems. This center coordinates efforts by the G-2/S-2, G-3/S-3, and G-6/S-6 to eliminate conflicts between battlespace functions. The EWCC is under staff cognizance of the G-3/S-3. Assigned personnel identify and resolve potential conflicts in planned operations. The EWCC includes an EWO, a communications system and information systems representative, and other liaison officers such as RadBn or VMAQ SMEs, Marine air control group radar officer, or representatives from other Services as needed.

MAGTF staffs will provide personnel to incorporate an EWCC with the Marine expeditionary force G-3/S-3. Personnel will also be provided for liaison teams to higher headquarters EW coordination organizations when required.

Electronic Warfare Addendums to the Operation Order

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

Appendix 2 (Signals Intelligence) to Annex B (Intelligence) of the OPORD contains specific instructions for SIGINT operations.

Operations Security

Operations security is the key to information denial. It gives the commander the capability to identify indicators that can be observed by the adversary's 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.

Operations security is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to—

- Identify those actions that can be observed by the adversary's intelligence systems.
- Determine indicators that the adversary's intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to the adversary.
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. For more information on operations security see JP 3-13.3, *Operations Security,* or MCWP 3-40.9, *Operations Security (OPSEC)*.

Operations Security in Support of the Offense

Although primarily associated with defensive measures, OPSEC contributes to the offense by depriving the adversary of information that slows the adversary's decision cycle, thereby providing opportunity for 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 adversary intelligence system, reducing its ability to orient combat power against friendly operations.

Operations Security Process

Operations security planning is accomplished through the OPSEC process. The OPSEC process has five distinctive steps that provide a framework for the systematic identification, analysis, and protection of information necessary to maintain essential secrecy (see JP 3-13.3):

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

Staff 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.

Support Agencies

The counterintelligence (CI)/human intelligence (HUMINT) teams perform a wide range of duties such as security briefings, countersabotage, counterespionage, and countersurveillance inspections. Counterintelligence measures enhance security, aid in reducing risks to a command, and are essential in achieving operational surprise during military operations. Counterintelligence

can provide a significant contribution to a unit's OPSEC program. Counterintelligence personnel can support a command's OPSEC program by conducting the following:

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

Normally, there is a CI/HUMINT company located within the intelligence battalion. Additional information on CI/HUMINT is provided in MCWP 2-6, *Counterintelligence*.

The Naval Criminal Investigative Service (NCIS) operates a worldwide organization to fulfill the investigative and counterintelligence responsibilities of the Department of the Navy. Within its 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 counterintelligence, assuming that NCIS assets are not locally available.

Operations Security and the Operation Order

Tab C (Operations Security) to Appendix 3 (Information Operations) 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.

Military Information Support Operations

Military information support 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 in a manner favorable to the originator's objectives. (JP 1-02)

At the strategic level, MISO may take the form of political or diplomatic positions, announcements, or communiques. At the operational level, MISO can include the distribution of leaflets, radio and television broadcasts, and other means of transmitting information that provide information intended to influence a selected group. It may be used to encourage adversary forces to defect, desert, flee, surrender, or take any other action beneficial to friendly forces. At the tactical level, MISO enables the tactical commander to directly communicate and empathize with target audiences. Tactical level MISO includes face-to-face contact and the use of loudspeakers or other means to deliver MISO messages.

Military information support operations shape attitudes and influence a foreign audience's behavior. The mere presence of Marine Corps forces may be a MISO activity in itself, bringing influence on a situation through a display of purpose. Military information support operations may also support military deception operations.

Integration

Military information support operations is only one of the means available to influence adversary attitudes and behaviors. When MISO is used concurrently with other information-related activities, it must be closely integrated with those capabilities in order to convey selected information in a synchronized way. Information operations personnel will coordinate public affairs (the delivery of the truth), OPSEC (the protection of friendly critical information), MILDEC (the concealment of friendly intentions and creation of misleading perceptions), and CMO (the delivery of friendly civil actions) with MISO operations.

Employment

During peacetime, MISO activities that support combatant commanders take the form of overt

peacetime MISO programs. These programs are proposed by combatant commanders through the Chairman of the Joint Chiefs of Staff (CJCS) 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 MISO 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 MISO plan is developed. Once a campaign plan is approved, the combatant commander or joint force commander is delegated MISO approval authority. This does not mean that the supported combatant commander has also been delegated approval for MISO product dissemination. In some cases, MISO products may be politically or religiously sensitive and may require separate approval for dissemination. The CJCS execute order, which is authorized by the Secretary of Defense, should designate who has authority for MISO product approval and who has authority for MISO product dissemination. The MAGTF's MISO actions must complement and support ongoing theater and joint force MISO activities.

The MAGTF will not normally identify, plan, or execute complex MISO activities; such as those requiring detailed theme development, intricate target analysis, or the use of sophisticated media. These missions will typically be conducted by external MISO units such as, a US Army military information support group (MISG), or US Air Force 193d Special Operations Wing. However, the MAGTF commander is responsible for providing MISO support and conducting tactical MISO (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 adversary. Marines execute observable actions that support psychological objectives.

The adversary is likely to employ MISO 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. The MAGTF's counteractions should be tailored to limit the adversary's opportunities to exploit the presence of Marines and their actions for MISO 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.

Military information support operations may be integrated as a nonlethal fire support asset and are planned by the G-3/S-3 and coordinated with public affairs and CMO.

Staff Responsibilities

Overall responsibility for the conduct of MISO falls under the cognizance of the G-3/S-3. The MISO officer is responsible to the G-3/S-3 for MISO planning and oversight. The MISO officer will write the MISO portion of the OPORD and coordinate and conduct approved MISO activities in support of tactical operations. If a designated MISO officer is not on hand, a MISO officer may be appointed to provide control and management of the MISO effort and to meet liaison requirements.

Additional Support

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

The Marine Corps has a limited-capability MISO section that is dedicated to conducting tactical MISO. The MISO section is located within the Marine Corps Information Operations Center. If required, additional MISO support may be provided by one of the US Army's MISGs.

The Army has the preponderance of MISO assets within DOD. There is one Active Component MISG with a worldwide capability under the US Special Operations Command (SOCOM) and three Reserve Component MISGs under the US Army Civil Affairs and Psychological Operations Command. A MAGTF serving as a JTF could potentially be augmented or supported by any number of US Army MISO elements from either the Active or Reserve Component.

Note: On 15 August 2011, the US Army directed the provisional establishment of the Military Information Support Operations Command (MISOC) with an initial operational capability to provide military information support forces to combatant commanders, US ambassadors, and other agencies in order to synchronize plans and to execute, inform, and influence activities across the range of military operations. The provisional status is expected to be rescinded in Fiscal Year 2014, when the Force Design Update is fully funded and implemented by the US Army.

The Air Force's 193d Special Operations Wing of the Pennsylvania Air National Guard flies the EC-130E Commando Solo. This provides an airborne radio and television broadcast capability that can be used for MISO purposes. The Active Air Force Component maintains additional dissemination capability for airborne leaflet drops.

Military Information Support Operations and the Operation Order

Tab D (Military Information Support Operations) of Appendix 3 (Information Operations) to Annex C (Operations) of the OPORD implements the recommended COA for MISO. Tab D details specific MISO tasks to be performed and specifies coordinating instructions for the control and management of MISO missions.

Cyberspace Operations

Cyberspace operations are one of the latest capabilities developed in support of military operations, which stems from the increasing use of networked computers and supporting information technology infrastructure systems by military and civilian organizations. In order to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure, cyberspace operations are used along with electronic warfare. For the purpose of military operations, cyberspace operations are divided into offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO):

- Offensive cyberspace operations are intended to project power by the application of force in or through cyberspace. (JP 1-02)
- Defensive cyberspace operations are passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 1-02)
- Cyberspace ISR is an intelligence action conducted by the joint force commander authorized by an executive order or conducted by attached signals intelligence units under temporary delegated signals intelligence operational tasking authority [SOTA] (see JP 3-12 for more information).
- Cyberspace operational preparation of the environment (OPE) consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations (see JP 3-12 for more information).
- Department of Defense information network operations are operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 1-02)

Due to the continued expansion of wireless networking and the integration of computers and radio frequency communications, there will be operations and capabilities that blur the line between cyberspace operations and EW and may require case-by-case determination when electronic warfare and cyberspace operations are assigned separate release authorities.

Staff Responsibilities

Cyberspace operations 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.

Cyberspace Operations Addendums to the Operation Order

Several appendices of the OPORD relate to cyberspace operations: Appendix 1 (Information Systems Security) to Annex K (Combat Information Systems) and Appendix 2 (Communications Security) to Annex K. Annex B (Intelligence) of the OPORD is the basic intelligence annex and contains elements related to cyberspace ISR and OPE; for example, Tab A (Communications Intelligence Collection Requirements) to Appendix 2 (Signals Intelligence).

Physical Attack

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

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

Rules of engagement 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 command and control elements of the adversary's C2 system. However, the adversary may be able to recover from physical destruction given sufficient time, resources, and redundancy. Planners should have some preplanned measure of effectiveness (MOE) to judge the results of physical destruction and be prepared to monitor targets after attack to determine their operational status. Critical adversary C2 nodes identified as effectively reconstituted should be considered for reattack if analysis determines that they are still operationally effective. Information operations integration with the BDA cycle is essential.

As an integrated part of information operations, physical attack is the systematic degradation or destruction of selected adversary C2 systems that allows the MAGTF to gain an informational advantage. Command and control nodes must be functionally destroyed. If an adversary C2 node receives only cosmetic structural damage, it may remain operational despite its structural damage. The adversary may be able to reconstitute C2 nodes and re-establish effective command and control via alternate means. Therefore, C2 targets may need to be attacked in depth to create desired effects. Restrike may be required to maintain suppression of adversary command and control.

However, the total destruction of the hostile C2 system may not be attainable or desirable. Friendly forces may need to use adversary 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*.

Tab E (Physical Attack) of Appendix 3 (Information Operations) to Annex C (Operations) of the OPORD is the physical attack/destruction tab. This tab implements the recommended COA for attack. Tab E 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

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. The security of friendly information and information systems is critical to gaining and maintaining information superiority. For more information on information assurance (IA), see JP 3-13, *Information Operations*.

Information assurance is actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 1-02) Information assurance capabilities include information security (INFOSEC), computer security, and COMSEC:

- Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and COMSEC.
- Computer security is the protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02)
- Communications security 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) Communications security 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. In order 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 systems 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 within the system administrator and user communities to mitigate system vulnerabilities, implement and maintain protected systems, and detect any attempts at exploitation.

Training and Certification

Headquarters, Marine Corps, Command, Control, Communications, and Comptuers oversees the Marine Corps Certification and Accreditation Program. The program is based on the Computer Security Act of 1987 (Public Law 100-235) requiring "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 of 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 Information Assurance Certificate can be awarded.

System Certification and Accreditation

All DOD information systems and networks will be certified and accredited in accordance with DODI [Department of Defense Instruction] 8510.01, *DOD Information Assurance Certification and Accreditation Process (DIACAP)*. Certification and accreditation of information systems that process Top Secret sensitive compartmented information will comply with the requirements of DCID [Director of Central Intelligence Directive] 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*.

Additionally, all Marines, Marine Corps civilian employees, and contractor personnel who perform Marine Corps duties in the administration of DOD computer systems in the Marine Corps enclave will be identified as either an information assurance manager (IAM) or information assurance technician (IAT), level 1, 2, or 3 in accordance with Department of Defense Directive 8570.01, *Information Assurance Training, Certification, and Workforce Management*. All personnel designated as an IAM or IAT are required to complete the appropriate certification level commensurate with their IAM or IAT classification in accordance with the guidelines set forth in Department of Defense Directive 8570.01.

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. These risks, once identified, must be categorized by severity and probability. Another important part of risk management is the development of means to mitigate those risks that may have severe impacts on the commander's desired end state.

Staff Responsibilities

Overall responsibility for the conduct of information assurance falls under the cognizance of the G-6/S-6. Defense of the network includes other discrete supporting functions, such as OPSEC, which are the responsibility of the G-3/S-3.

Support Agencies

The Marine Corps Network Operations and Security Center (MCNOSC) is located in Quantico, VA. The MCNOSC provides continuous, secure, global communications and operational sustainment and defense of the Marine Corps Enterprise Network (MCEN) for Marine Corps forces worldwide in order to facilitate the exchange of information across the defense information infrastructure. The MCNOSC exists to supply customer support to the MCEN and maintains a 24/7 helpdesk.

The responsibility of all Marines to report a virus hit or a threatening attempt to access a system is crucial. Because an attempt on a Marine Corps system could be part of a larger, overall attempt to disrupt or exploit Marine Corps information systems, the attempted breach can only be discovered and defended against if all attempts are reported. When a virus or attempted compromise occurs, the local IAM is contacted to obtain immediate assistance. Initial reports are initiated according to the local/regional base or station's guidance. At minimum, the MCNOSC help desk is contacted to report the incident.

The Service computer emergency response team for the Marine Corps is the Marine Corps Computer Emergency Response Team (MARCERT), which is an element of the MCNOSC 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 Corps force DCO 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.

Joint Task Force–Global Network Operations (JTF-GNO) serves as the focal point within 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-GNO is responsible for DOD-wide recovery operations to stop or contain damage and restore network functions to DOD operations. The JTF-GNO is collocated with, and supported by, the Defense Information Systems Agency (DISA) in order to take advantage of the existing operational computer network capabilities of DISA's Global Operations and Security Center.

Defense Information Systems Agency operates a program known as the DISA Vulnerability Analysis and Assistance Program, which specifically focuses on automated information system vulnerability. Upon customer request, this program collects, identifies, analyzes, assesses, and resolves INFOSEC vulnerabilities.

The National Security Agency has a COMSEC monitoring program that focuses on telecommunications 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 of INFOSEC measures 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.

Marine Corps Intelligence Activity is the first line of defense with relation to the certification and accreditation of information systems that process Top Secret sensitive compartmented information within the Marine Corps operating structure. Marine Corps Intelligence Activity is also the first point of contact for issues dealing with DCO in the sensitive compartmented information computing environment.

Information Assurance Addendums to the Operation Order

Appendix 1 (Information Systems Security) to Annex K (Combat Information Systems) of the OPORD is the IA appendix. This appendix implements the recommended COA for information assurance. It details specific tasks to be performed and specifies coordinating instructions for the control and management of information assurance.

Physical Security

Physical security is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02)

Physical security contributes directly to information protection. Information, information-based processes, and information systems—such as C2 systems, weapon systems, and information infrastructures—are protected relative to the value of the information they contain and the risks associated with the compromise or loss of information. For more information on physical security see JP 6-0, *Joint Communications System*.

Staff 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.

Physical Security Addendums to the 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 (Communications Security) to Annex K (Combat Information Systems) of the OPORD.

Counterintelligence

Counterintelligence is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. (JP 1-02)

Counterintelligence 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. The principal objective of counterintelligence is to assist with protecting friendly forces. Counterintelligence 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 organization or efforts.

Counterintelligence provides critical intelligence support to command force protection efforts by helping identify potential threats, adversary 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. Counterintelligence increases uncertainty for the adversary, thereby making a significant contribution to the success of friendly operations. Counterintelligence also identifies friendly vulnerabilities, evaluates security measures, and assists with implementing appropriate security plans. Physical security reduces vulnerability. Operations security reduces exposure. The integration of intelligence, counterintelligence, and operations culminates in a cohesive unit force protection program. See MCWP 2-6.

Staff 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 system security.
- G-1/S-1: information and personnel security.
- Headquarters commandant: physical security.

Counterintelligence Addendums to the Operation Order

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

Public Affairs

Public affairs are those public information, command information, and community engagement activities directed toward both the external and internal publics with interest in the Department of Defense. (JP 1-02) The Marine Corps PA mission is to communicate and engage; building an understanding, credibility, trust, and mutually beneficial relationships with domestic and foreign publics on whom the Marine Corps' mission success or failure depends.

Public affairs methods range from direct communication with key publics, such as face-to-face engagement or social media outreach, to indirect communication through traditional media channels or other third parties. Additionally, public affairs provides the MAGTF commander a means by which to communicate with all publics since public affairs can legally engage American, international, and host-nation audiences, as well as friendly, neutral, or adversary audiences.

In its operational role, MAGTF PA efforts have impacts within the battlespace that may often have a strategic effect on the mission. As such, public affairs and information operations are considered related activities that contribute significantly to the commander's communication strategy. While PA and IO are separate functional areas for authoritative and organizational purposes, each directly supports military objectives, counters adversary propaganda and misinformation, and deters adversary actions. Effective employment of both requires planning, message development, and media analysis; but, each effort may differ with respect to audience, scope, and intent. For maximum effectiveness, PA and IO planners will coordinate their efforts and deconflict activities consistent with DOD principles of information, organizational policy, statutory limitations, and OPSEC. Commanders, therefore, must ensure continual collaboration between PA and IO activities as part of operational planning. (For more information, see MCWP 3-33.3, *Marine Corps Public Affairs*.)

Enlisted PA Marines, called combat correspondents, are trained still photographers, videographers, and writers who can support the MAGTF across the range of military operations and can aid the IO officer by creating truthful content and communication products for dissemination. Public affairs Marines also possess dissemination capabilities that can help the MAGTF transmit first truth accounts from the battefield or operating environment to key publics.

Public Affairs, Military Information Support Operations, and Civil-Military Operations

In an expeditionary setting, public affairs, MISO, and CMO all may disseminate information to local populations. Public affairs elements have primary responsibility for dealing with news media outlets and will assist the other functions in passing information to the public through appropriate news outlets. However, MISO and CMO are not otherwise restricted from using other available message channels to disseminate their message, to include electronic media. Public affairs efforts that may affect MISO and CMO missions include electronic information activities, imagery release, and news media engagement. Accordingly, MISO, CMO, and PA planners

must actively coordinate within the IO working group or cell or coordinate directly when there is no IO coordination capability established.

Public Affairs and Military Deception

Public affairs should plan, coordinate, and deconflict with MILDEC operations consistent with policy, statutory limitations, and operations security. The primary purpose of this coordination is to safeguard essential elements of friendly information and preserve the effectiveness of deception efforts. The public affairs officer is responsible to ensure that PA actions related to MILDEC maintain the integrity, reputation, and credibility of public affairs as a source for truthful information.

Public Affairs, Cyberspace Operations, and Electronic Warfare

Various PA activities, such as facilitating embedded news media access, are often impacted by cyberspace operations and EW capabilities. Public affairs officers are responsible for coordinating with cyberspace operations and/or EW activities within the IO working group or cell in order to ensure PA operations are not inadvertently affected.

Staff Responsibilities

Public affairs is a command responsibility and a function of command and control and is considered a special staff function executed by the MAGTF PAO.

Public Affairs Addendums to the Operation Order

The PAO participates in the MCPP to ensure PA considerations are included in problem framing, COA development and selection, and are integrated into the OPORD. Throughout the planning process, the PA planner contributes to the development of the combined information overlay, and he also develops, uses, and updates the PA estimate, the PA guidance (if developed already), and Annex F (Public Affairs) of the OPORD. Annex F defines the PA mission, articulates communication goals, details specific PA tasks, identifies communication assumptions, and specifies coordinating instructions for the control and management of PA efforts.

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 is the designated Active and Reserve component forces and units organized, trained, and equipped specifically to conduct civil affairs operations and to support civil-military operations. (JP 1-02)

Each military operation has a civil dimension. The civil dimension requires commanders to 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 adversary, meeting legal and moral obligations to civilians, and providing access to additional capabilities.

Civil-military operations 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 and are involved in multinational training activities and exercises that contribute to international cooperation and stability. The Marines respond to complex emergencies, such as natural disasters, that overwhelm civil authorities and they 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 peaceful transition of control back to civil authorities.

In most cases, Marines will operate in close contact with civilians and their governments. They carefully develop, nurture, and maintain positive relations between the people, governments, and nongovernmental organizations 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 vary during each operation and throughout the various phases of each operation. Civil-military operations 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. Civil-military operations are conducted to facilitate military operations, achieve military operational objectives, and satisfy US policy goals. For more detailed information on CMO see JP 3-57, *Civil-Military Operations*, and MCWP 3-33.1, *Marine Air-Ground Task Force Civil-Military Operations*.

Civil affairs describes designated personnel and distinct units. It is neither a mission nor an objective, but the name of a particular force that assists the MAGTF commander in planning, facilitating coordination, and conducting CMO. Expertise is available to CA forces that is not normally available to the MAGTF, they are organized and equipped specifically to support CMO. Civil-military operations 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. Civil-military operations occur throughout the planning and execution of military operations and are not merely an adjunct specialty that occurs before or after hostilities. Civil affairs operations (CAO), however, are distinguishable from CMO to the extent that CAO are characterized by the application of functional specialties in areas that are normally the responsibility of the local government or civil authority. Civil affairs operations are accomplished by functional specialists with the requisite MOS [military occupational specialty], and they reside in the Army Reserve Component only. The Marine Corps only has two legal and public health functional specialists within the Reserve Component. Although the Marine Corps does limited CAO and can certainly leverage support from the whole of government to do it when required, the Marine Corps is not manned, trained, or equipped to specifically conduct CAO.

Civil-miliary operations, executed by all members of the MAGTF, may include performance by military forces of activities and functions normally the responsibility of local government.

Civil-military operations can assist to support friendly or host-nation civilian welfare, security, and developmental programs, and CAO 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 MCWP 3-33.1.

Tasks

Civil-military operations focus on the relationship between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in areas where military forces are present. While executing CMO, the MAGTF is responsible for five core tasks:

- Facilitating populace and resources control.
- Facilitating foreign humanitarian assistance.
- Facilitating nation assistance.
- Managing civil information.
- Facilitating support to civil administration responsibilities.

Staff Responsibilities

Civil-military operations are a function of operations. The CA officer normally operates under the staff cognizance of the G-3/S-3. However, if 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 Information Management

Civil information management is the process that includes the planning, collection, analysis, and production of civil information that is consolidated in a central database and shared with the supported elements, higher headquarters, other US Government and DOD agencies, international organizations, and nongovernmental organizations. Civil affairs teams and all Marines within the MAGTF will conduct civil reconnaissance and push/pull civil information such as ASCOPE [areas, structures, capabilities, organizations, people, and events] and PMESII [political, military, economic, social, information, and infrastructure] to higher headquarters. Information operations, as well as all other warfighting functions, can use this information and analysis in their planning process and make better informed recommendations to the commander.

Civil-Military Operations Addendums to the Operation Order

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

Combat Camera

Combat camera is the acquisition and utilization of still and motion imagery in support of operational and planning requirements across the range of military operations and during exercises. (MCRP 5-12C) Official visual documentation is used for operational and combat support as well as public information purposes. It is an essential visual record of Marine Corps commands throughout significant and often historical events. Complete access to areas of operations and timely exploitation of collected imagery are key to COMCAM success. For more information on COMCAM, see MCWP 3-33.7, *MAGTF Combat Camera*.

The mission of COMCAM is to provided the President, Secretary of Defense, CJCS, Military Departments, combatant commanders, and on scene commander with a directed image capability in support of operational and planning requirements during world crisis, contingencies, exercises, and wartime operations. (Marine Corps

Order 3104.1_, *Marine Corps Combat Camera Program*) Combat camera is a fundamental tool of commanders and decisionmakers and—

- Provides commanders with combat trained documentation teams that are primarily suppliers of operational imagery.
- Supports combat, information, humanitarian, special force intelligence, surveillance, and reconnaissance (ISR); engineering; legal; and PA missions.
- Provides valuable imagery, simultaneously, at the strategic, operational, and tactical levels of war.
- Speeds decisionmaking and facilitates the execution of missions at lower levels through vertical and horizontal information flow.

Marine Corps COMCAM teams are organized, trained, and equipped to provide rapid deployment of COMCAM assets in support of exercises, operations, and contingencies that support the operating forces and are available for tasking by—

- The Secretary of Defense, the CJCS, and Federal agencies as directed.
- Unified and subunified combatant commanders.
- Joint and combined task force commanders and their staffs.
- Marine Corps component commanders and their staffs.

Challenges faced by commanders on today's battlefields make COMCAM operations more critical and difficult to execute. Commanders will exploit imagery at various times and various sources such as ISR, public affairs, coalition forces, or civilian media. Therefore, MAGTF COMCAM Marines must be prepared to incorporate COMCAM assets into missions across the full range of military operations and be flexible to task-organize COMCAM for any size MAGTF and operation.

The COMCAM Marines support a commander's situational awareness, IO, PA, and CA objectives to include ISR, BDA, MILDEC, legal, and history functions. Combat camera supports the commander's imagery requirements and produces timely products supporting the commander's intent and mission objectives.

The MAGTF COMCAM officer serves as a battlestaff officer who advises the MAGTF commander on issues, capabilities, and requirements pertaining to COMCAM operations. Normally assigned to the assistant chief of staff, G-3, or the IO cell, the COMCAM officer manages all the MAGTF commander's COMCAM assets to include table of organization, table of equipment, and augmentation tasks from higher command; task-organizes COMCAM personnel for any operational commitments; and develops Marine expeditionary force/Marine expeditionary brigade operational annexes and OPORDs pertaining to COMCAM.

Combat camera personnel are assigned to the Marine expeditionary unit command element. Additional assets within ground combat element, aviation combat element, and logistics combat element support these personnel based on requirements. Regardless of size, COMCAM units maintain the capability to acquire, edit, disseminate, archive, manage, and transmit imagery. All COMCAM units are equipped to acquire imagery in darkness and inclement weather.

Defense Support to Public Diplomacy

Defense support to public diplomacy consists of activities and measures taken by DOD components, not solely in the area of information operations, to support and facilitate the public diplomacy efforts of the US Government.

Department of Defense contributes to public diplomacy, which includes those overt international information activities of the US Government designed to promote US foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers

and by broadening the dialogue between American citizens and institutions and their counterparts abroad. When approved, MISO assets may be employed in support of defense support to public diplomacy as part of security cooperation initiatives or in support of US embassy public diplomacy programs. Much of the operational level IO activity conducted in any theater will be directly linked to public diplomacy objectives. Defense support to public diplomacy requires coordination across US Government departments and agencies, and amongst all DOD components.

This Page Intentionally Left Blank

CHAPTER 4
INFORMATION OPERATIONS INTELLIGENCE INTEGRATION

Critical to the planning, execution, and assessment of information operations is information operations intelligence integration (IOII). Information operations require accurate, timely, and detailed intelligence if it is to be successful. Early integration between Marine IO staffs involved in planning and executing IO actions and IOII staffs is imperative. The complex nature of the information environment levies requirements on the intelligence cycle not normally associated with normal operational planning. Information operations planners must understand that limited intelligence resources, legal constraints, long lead times, and the dynamic nature of the information environment have an affect on IOII. The IO requirements are almost limitless, while collection resources are limited. The information environment changes over time according to different factors. The intelligence needed to affect adversary or other target audience decisions often requires specific sources and methods to be positioned and employed over a long period of time to collect and analyze the needed information.

In order to effectively engage the intelligence system, the IO staff should clearly articulate intelligence requirements so that the G-2/S-2 staff can effectively work on behalf of the IO staff. The IO staff should establish relationships with the G-2/S-2 staff that will facilitate successful IO planning and execution initiatives.

Information operations intelligence integration is conducted as part of the IPB process. The same four-step IPB process that is used for traditional operations is also used for information operations:

- Define the battlespace environment.
- Describe the battlespace effects.
- Evaluate the adversary.
- Determine adversary COA.

The primary difference between IPB for traditional operations and IO is the focus and the degree of detail required. Intelligence preparation of the battlespace is critical for the conduct of information operations in support of stability operations, civil support operations, and counterinsurgency operations.

The function of intelligence for information operations in support of counterinsurgency is to understand the operational environment/battlespace environment, with emphasis on the local population, host nation, and insurgents. Commanders and planners require insight into cultures, perceptions, values, beliefs, interests, and decisionmaking processes of individuals and groups. An early analysis of a key target audience's information environment must be conducted prior to the execution of any detailed planning efforts. This analysis continues throughout the planning and execution in order to achieve a better visibility and understanding of that information environment. These requirements are the basis of collection and analytical efforts.

Information operations intelligence integration in support of stability operations or defense support of civil authorities operations utilizes IPB that integrates adversary doctrine and operational patterns with terrain, weather, and civil considerations such as cultural, religious, ethnographic, political, social, economic, legal, criminal, and demographic information. Intelligence preparation of the battlespace relates these factors to the specific mission and situation. See MCRP 2-3A, *Intelligence Preparation of the Battlefield/*

Battlespace, for further information on IPB in support of these operations.

Intelligence Support to Assessments

Intelligence support to information operations presents new and unique challenges to intelligence professionals throughout the PDE&A [planning, decision, execution, and assessment] cycle because information operations must be worked in ways that do not fit neatly into the patterns applied in other forms of intelligence support. This is true in the combat assessment phase and its subsequent impact on the collection phase. Early in planning, operations and intelligence personnel must develop MOEs and tailor an intelligence collection plan that adequately assesses those MOEs. Measures of effectiveness are continually refined throughout the process so that the impact of operations on the information environment can be evaluated. Analysts must have a major role in defining suitable MOEs for specific IO actions in order to properly resource collection assets.

Intelligence analysts help assess task accomplishment by supporting MOE, measure of performance, and reattack recommendations. At the strategic and operational levels, IPB products provide much of the substantive baseline analysis and characterization of systems and functional capabilities required for target system analysis and task assessment. At the operational level, the IPB process supports target development by determining the anticipated times and locations where adversary targets are expected to appear. At the tactical level, IOII support may also include analysis of specific target composition and vulnerability. This data enables target systems analysts to develop the specific battle damage indicators and measures of performance to assess task accomplishment. Intelligence professionals must work with operators to establish IO MOEs, and must seek to develop and apply intelligence efforts in the fields of signals and HUMINT earlier in the planning process. Collection must be tailored to evaluate MOEs to aid the commander making operational decisions.

Intelligence Support to Operations Security

An adversary will seek to collect critical information in order to achieve an operational advantage. Critical information consists of the significant information and indicators that can be used by the adversary to gain real advantage, decisively assure success, or preclude failure. Operations security, an operations function, seeks to reduce or deny the adversary's ability to collect information concerning friendly dispositions, capabilities, vulnerabilities, and intentions regarding both training and operations.

Intelligence support to OPSEC will focus on analysis of the adversary's ability to collect against friendly forces. Intelligence efforts involve the research and analysis of intelligence, counterintelligence, and open source information to identify the likely adversaries within the planned operation. Once identified, intelligence personnel will analyze and interpret collected information to identify indications of how an adversary could collect critical information and will seek to understand the adversary's decision cycle and any bias towards certain friendly information/intelligence collectors or disciplines.

Intelligence personnel also will assist operations in assessing friendly vulnerabilities and an adversary's ability to exploit those vulnerabilities in order to counter command implemented OPSEC measures. In addition, they will recommend physical and virtual offensive and defensive methods that will degrade an adversary's communications systems and ISR capabilities.

Intelligence Support to Military Information Support Operations

Military information support operations are an operations function that aims to influence adversary attitudes and behavior, thereby affecting the achievement of military objectives. Effective MISO can degrade adversary command and control. The MISO staff works closely with the intelligence staff to plan MISO and effectively integrate these with the other IO elements. Operations security may be essential to the MISO plan. Equally, it may be desirable in support of MISO to reveal certain aspects of friendly dispositions, capabilities, and intentions for MILDEC purposes.

Intelligence support to MISO includes identifying target audiences and other groups, their locations, conditions, strengths, vulnerabilities, susceptibilities, political environment, cultural environment, cultural norms, values, perceptions, attitudes, public opinion, tribal connections, alliances, beliefs, ideology, and behaviors. Several organizations (including Marine Corps Intelligence Activity, the Defense Intelligence Agency, and the Joint Information Operations Warfare Command) 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 conditions and attitudes of target groups are likely to change as the situation develops. Current all-source intelligence, in particular HUMINT and SIGINT, is vital in the planning phase and throughout the execution of MISO. Intelligence will help assess the effectiveness of current MISO activites, reinforce success and assist the commander in the allocation of limited resources. The intelligence staff also monitors the effect of the adversary's MISO on the MAGTF force in order to support defensive operations. Counterintelligence provides intelligence on subversion (and can be tasked to counteract subversion), which forms part of the adversary's MISO campaign.

Intelligence Support to Deception

Deception is an operations function that aims to present a deliberately false picture to the adversary to cause him to act contrary to his interests and in favor of the commander's objectives. Deception is highly complex, in particular those aspects that seek to exploit adversary command and control, and it demands security at the highest level. Operations security is essential to deception, because it conceals those aspects and indicators that would allow the adversary to determine the reality behind the deception.

Deception uses selected conduits, identified by intelligence, to feed information to the targeted adversary decisionmaker. Electronic warfare, cyberspace operations, counterintelligence, 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 electronic attack or physical attack. Intelligence must monitor and support the identification of deception conduits as well as conduits targeted with electronic attack, cyberspace operations, or physical attack.

Intelligence supports deception by identifying the capabilities and limitations of the adversary's intelligence-gathering systems as well as the adversary's biases and perceptions. This requires the identification of the adversary's decisionmaking processes and patterns. The analysis of the

capabilities and limitations of the adversary's CI and security services is also required.

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.

Intelligence Support to Electronic Warfare

The interception, identification, analysis, and, where possible, the understanding of the adversary's electromagnetic spectrum 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 in order 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 command and control must be based on an assessment of the balance between destruction, neutralization, and exploitation, and between hard-kill and soft-kill methods. For example, in order to support the electronic deception plan, it may be necessary to ensure that certain adversary EW support systems are protected from attack. 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.

Intelligence Support to Physical Attack

Information operations intelligence integration should not be considered as supporting only nonlethal actions. Information operations has an extremely important function in supporting attacks that cause physical destruction, but can only be effective if strongly supported by intelligence resources. Careful intelligence integration can determine what targets to select for physical destruction and whether such an attack will support, or hinder, the effect a commander wants to create on a target audience. The target audience may be a decisionmaker whose decisions can impact a commander's end state or others who are influenced by that decisionmaker. A target can be a system that supports the flow of information to a decisionmaker, a person who provides advice and counsel to that decisionmaker, or a mechanism that allows a decisionmaker to project information.

Intelligence support can help determine the proper target and how its removal or degradation will impact the decisionmaker by—

- Assessing if a physical attack will create or alter perceptions, interrupt the flow of information forcing a decisionmaker to make decisions based on incomplete information.
- Driving an adversary to use certain exploitable information systems.
- Preventing the projection of an adversary's propaganda.
- Removing decisionmakers resulting in a disruption in an adversary's chain of command.

Likewise, it can assess the second and third order effects the attack may produce on different target audiences. Information operations intelligence integration support to physical attacks must work in conjunction with IO planners and be fully integrated into the targeting cycle.

Targeting and Enabling Support to Cyberspace Operations

Cyberspace operations consist of OCO, DCO, cyberspace ISR, cyberspace OPE, and Department of Defense information network operations. Cyberspace ISR and OPE are conducted pursuant to military authorities and must be coordinated and deconflicted with other US

Government departments and in accordance with the Department of Defense, the Department of Justice, and the intelligence community agreements and Executive Order 12333, *United States Intelligence Activities*. Cyberspace ISR includes ISR activities in cyberspace conducted to gather intelligence from target and adversary systems that may be required to support future operations, including OCO or DCO. These activities synchronize and integrate the planning and enable operation of cyberspace sensors; assets; and processing, exploitation, and dissemination systems in direct support of current and future operations. Cyberspace ISR focuses on tactical and operational intelligence and on mapping the adversary's cyberspace to support military planning. Cyberspace ISR requires appropriate deconfliction and cyberspace forces that are trained and certified to a common standard with the intelligence community.

Cyberspace OPE seeks to gain and maintain access to systems and processes and to position capabilities to facilitate follow-on actions. This includes identifying data, software, system/network configurations and identifiers, or physical structures connected to (or associated with) the network for the purposes of determining system vulnerabilities, actions taken to assure future access and/or control of the system, network, or data during anticipated hostilities (e.g., tagging malware for recognition by network defenses, delivering dormant payloads for future activation). Cyberspace OPE requires cyberspace forces trained to a standard that prevents compromise of related intelligence community operations.

Cyberspace ISR and OPE are critical enabling activities supporting OCO and DCO. The RadBn and Marine cryptologic support battalion are organic, major contributors of intelligence information supporting cyberspace operations. The Marine Corps Service component in US Cyber Command provides additional support to cyberspace operations. All cyberspace ISR efforts conducted by tactical units must be coordinated and deconflicted with other US Government departments and appropriate national agencies and the IO cell of the supported and/or higher unit.

Intelligence support to cyberspace operations requires an assessment of adversary information capabilities including friendly systems likely to be targeted by the adversary; the adversary's ability to exploit friendly systems; the adversary's ability to detect, attribute, and mitigate operations against their network and likely COAs.

Intelligence Support to Information Assurance

A coordinated IA plan to protect friendly C2 systems from adversary attack will make an adversary's information operations more difficult. Information operations 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.

This Page Intentionally Left Blank

APPENDIX A
INFORMATION OPERATIONS CELL RESPONSIBILITIES

The IO cell is composed of intelligence personnel, augmentees supporting IO activities, representatives from staff elements, and SMEs from appropriate warfighting functions. The size and structure of the cell is tailored to the mission and the commander's intent. The IO cell is responsible for the following:

- Planning the overall IO effort including preparing Appendix 3 (Information Operations) to Annex C (Operations), to the MAGTF OPORD.
- Coordinating to ensure synchronization with Annex F (Public Affairs), Annex G (Civil-Military Operations), Annex K (Combat Information Systems), Annex S (Special Technical Operations), and Annex U (Information Management).
- Developing IO concepts of support.
- Recommending IO priorities.
- Coordinating subordinate IO plans.
- Coordinating the planning and execution of IO activities between organizations responsible for each IO element.
- Coordinating nodal analysis and compiling IO target list.
- Submitting IO targets for inclusion in MAGTF targeting plans.
- Ensuring the OPSEC plan provides necessary command and control and communications protection and is coordinated with the deception plan and operations.
- Ensuring that other IO elements support the deception effort.
- Ensuring MISO themes support, and are supported by, the other IO elements.
- Coordinating IO intelligence integration.
- Coordinating and deconflicting IO with STO.
- Recommending additions, deletions, and modifications to rules of engagement.
- Coordinating EW and cyberspace operations actions with the appropriate staff planner.

Information Operations Officer

The IO officer is responsible to the commander via the G-3/S-3 for synchronizing IRCs that support IO tasks. He also has the following responsibilities:

- Establishes the IO working group (IOWG) to coordinate, synchronize, and integrate IO efforts and develops measurements of effectiveness and performance in order to assess the effectiveness of IO actions.
- Owns no assets and must work with the staff in order to integrate information operations into planning functions.
- Ensures IO representation and input are provided to MAGTF OPT.
- Ensures the staff understands the IRCs and limitations.
- Identifies the commander's end state in conjunction with the command's planning efforts and formulates an IO plan and/or IO concept of support to achieve end state.
- Is responsible for preparing the IO annex to the OPORD.
- Assists in the integration and synchronization of the execution of IO actions.
- Determines the effectiveness of the IO concept of support and makes recommendations to the G-3/S-3 to adjust accordingly.
- Oversees personnel within the IO cell and calls plenary IO cell meetings to include external support augmentees as appropriate.

- Coordinates all IO matters with higher, adjacent, and subordinate units.
- Requests external support from and coordinates IO activities with IO organizations such as Joint Information Operations Warfare Center, Joint Warfare Analysis Center, National Security Agency, and Defense Intelligence Agency, as required.

Intelligence (G-2/S-2) Member

The G-2/S-2 member provides timely and directed IO intelligence integration and has the following responsibilities:

- Coordinates the development and prioritization of IO intelligence requirements.
- Satisfies IO intelligence requirements through the fusion of all-source intelligence to include open source.
- Provides an information environment assessment of the area of operations and continually refines that assessment.
- Identifies target audiences/potential actors whose decisions may impact a commander's end state.
- Recommends methods that will impact an adversary's ability to collect, protect, or project information.
- Provides intelligence gain/loss analysis and reconciles restricted C2 targets on the restricted frequency list.
- Assists in the development of measures of effectiveness and coordinates mechanisms needed to collect the required data to determine the level of success of the IO concept of support.
- Coordinates with intelligence analysts to identify collection requirements based on specific needs identified by the IO cell.
- Coordinates development of targeting products to support IO planning.
- Assists with the preparation of IO portions of MAGTF operation plans.
- Informs MAGTF G-2s/S-2s of IO planning or execution activity to engage appropriate ISR capabilities for targeting and impact assessment.
- Provides assistance (through the IO cell) in assessing the operational impact and recommends appropriate recovery/response actions for computer intrusions affecting MAGTF computer infrastructures in support of the G-6/S-6 mission supporting information assurance.
- Coordinates COMSEC monitoring support in concert with G-3/S-3 and G-6/S-6 from the Joint Communications Security Monitoring Activity (JCMA), including JCMA's force protection communications support and the RadBns, during operations and exercises.
- Identifies areas of OPSEC concern for JCMA and the RadBn focus.
- Integrates COMSEC monitoring activities with trusted agents for other IO activities; such as, MISO, deception, OPSEC, and CI functions to enhance IO efforts.
- Identifies, in coordination with headquarters staff representatives, critical MAGTF information resources outside the MAGTF area of operations.
- Prepares notification messages for supporting commands or agencies to highlight the need to monitor and protect critical nodes.
- Participates in the IOWG, as required.

Communications System (G-6/S-6) Member

The G-6/S-6 member provides information on signal security and COMSEC efforts and recommends adjustments. The G-6/S-6 also has the following responsibilities:

- Identifies critical command and control and communication system nodes for protection.
- Provides protected and restricted frequencies to the restricted frequency list.
- Coordinates and reports on JCMA monitoring of MAGTF communications architecture.
- Participates in the IOWG, as required.

Operations Security Officer

The OPSEC officer oversees overall OPSEC efforts and is responsible for the following:

- Develops and updates the OPSEC plan.
- Initiates an OPSEC feedback program to monitor OPSEC effectiveness.
- Coordinates all OPSEC activities with external agencies and organizations.
- Participates in the IOWG, as required.

Military Information Support Operations Officer

The MISO officer maintains a thorough knowledge of all MISO plans and actions. He also is responsible for the following:

- Provides expert advice on MISO matters.
- Coordinates MISO plans, actions, and support with other IO elements, especially OPSEC and deception.
- Participates in the IOWG, as required.

Deception Officer

The deception officer heads the deception cell and has the following responsibilities:

- Coordinates development and update of deception plan, including obtaining higher-level authority if required.
- Monitors and controls dissemination of deception-related information; ensures security of material is maintained.
- Coordinates deception plans with other IO elements.
- Coordinates with the G-2/S-2 for feedback on deception success.
- Monitors and controls execution of the deception event schedule.
- Participates in the IOWG, as required.

Electronic Warfare Officer

The EWO oversees the EWCC under the direction of the G-3/S-3 and has the following additional responsibilities:

- Prepares EW plans.
- Coordinates EW operations with internal units and external agencies.
- Coordinates EW operations with other IO elements.
- Establishes and maintains the restricted frequency list with the G-6/S-6.
- Participates in the IOWG, as required.

Cyberspace Operations Officer

The cyberspace operations officer plans and coordinates offensive cyberspace, defensive cyberspace, cyberspace ISR, cyberspace OPE, and Department of Defense information network operations with internal units and external agencies. He also coordinates cyberspace operations with other IO elements and US Government departments and agencies, and participates in the IOWG, as required.

Special Technical Operations Officer

The STO officer plans, coordinates, and deconflicts STO activities. He also has the following responsibilities:

- Ensures the IO cell is aware of STO activities as required.
- Conducts liaison with higher STO representatives to facilitate coordination and release and execution authority for STO.
- Participates in the IOWG, as required

Public Affairs Officer

The PAO provides advice to the IO cell on all PA matters and ensures PA considerations and themes support and are supported by the IO plan. The PAO also coordinates PA plans, actions, and

programs with IO efforts with particular emphasis on MISO, OPSEC, EW, and MILDEC activities.

Targeting Representative

The targeting representative provides entry for IO targets into the targeting cycle and is responsible for the following:

- Ensures IO targets are given proper consideration in the targeting process.
- Provides IO cell recommendations to the restricted target list.
- Participates in the IOWG, as required.

Counterintelligence Officer

The CI officer assesses defensive IO posture from a CI perspective and recommends corrective actions. The CI officer also participates in the IOWG, as required.

Other Representatives

Other IO cell members have the following responsibilities:

- Attends IO cell sessions as invited by IO officer.
- Provides expert advice and opinions.
- Coordinates with parent organizations in support of MAGTF IO.
- Participates in the IOWG, as required.
- Conduct legal analysis of proposed operations within the context of applicable laws and authorities.

APPENDIX B
INFORMATION OPERATIONS PLANNING PRODUCTS

Information Operations

The staff estimate for information operations is an estimate focused on the information environment and the use of information by adversary and friendly forces. It assesses the situation in the information environment and analyzes the best way to achieve information superiority for the assigned mission. See figure B-1 on page B-2.

Combined Information Overlay

The impact of the information environment should be analyzed to consider how significant characteristics affect friendly, neutral, and adversary capabilities and broad COAs. Significant characteristics, further analyzed within the physical, informational, and cognitive dimensions, can be graphically represented on a combined information overlay (see fig. B-2 on page B-3). The analyst can use this overlay to identify strengths and/or vulnerabilities within the information environment that can be exploited by friendly or adversary forces. The intelligence analyst works closely with the IO officer to ensure the combined information overlay is continually updated throughout the planning process.

Information Operations Concept of Support

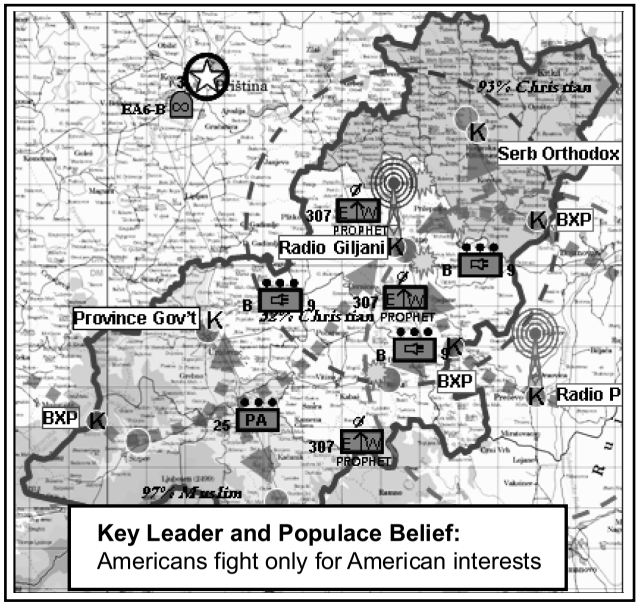
The information operations concept of support shown in figure B-3, on page B-4, describes how available forces will achieve information superiority. It states when and where information superiority needs to be achieved and describes how information operations will support the operation and how information operations capabilities will be employed. Information operations personnel develop an IO concept of support for each assigned mission or COA based on what the command's assets and resources can do to achieve the IO objectives.

Sub-IE: North
Populace: Supports adversary, multiple rural TAs
Info Flow: Cell phone, internet, TV, radio
Info Infrastructure: Well-developed and multiple conduits, supports adversary C2
COA Considerations: Adversary propaganda flow
Conditions: Inner LOCs favor adversary

Sub-IE: Central
Populace: Supports government, urban hubs
Info Flow: Multimedia, cell phone, broadcasts affected by CF versus border state
Info Infrastructure: Unreliable, frequent power outages, follows main LOCs
COA Considerations: Adversary focus, intimidation main effort
Conditions: Favor friendly forces

Sub-IE: South
Populace: Supports government, rural strong tribal/clan links
Info Flow: Slow, F2F, TV, radio
Info Infrastructure: Dilapidated, unreliable, frequent power outages, follows main LOCs
COA Considerations: Area is an information vacuum, requires multiengagements
Conditions: Favor friendly forces

Adversary
Collect:
Capabilities: HUMINT, SIGINT
Vulnerabilities: Loyalty of followers, cell paranoia
Recent Activity: Penetration of local police
Protect:
Capabilities: Intimidation of populace
Vulnerabilities: Couriers, internet, cell phones
Recent Activity: Unsecure communications
Project:
Capabilities: F2F, radio, internet
Vulnerabilities: C2
Recent Activity: Anti-US themes
Likely COA: Incite civil unrest in center of AOR, discredit CF actions; build legitimacy/recruit with local militia



Friendly
Organic:
EA: 307 EA Prophet
PA: 25 PA
MISO: 1 3
Supporting:
EA: 3 EA6-B

Vulnerabilities:
- Non-secure handheld radios

COA Considerations:
- Intel loss versus gain with EA
- Interdict border state info flow

LEGEND

AOR	area of responsibility	**F2F**	face to face	**Intel**	intelligence
BXP	border crossing point	**Govt**	government	**LOC**	line of communications
CF	coalition force	**IE**	information environment	**MISO**	military information support operations
EA	electronic attack	**Info**	information	**TV**	television

Figure B-1. Example of a Staff Estimate for Information Operations: Graphical Display.

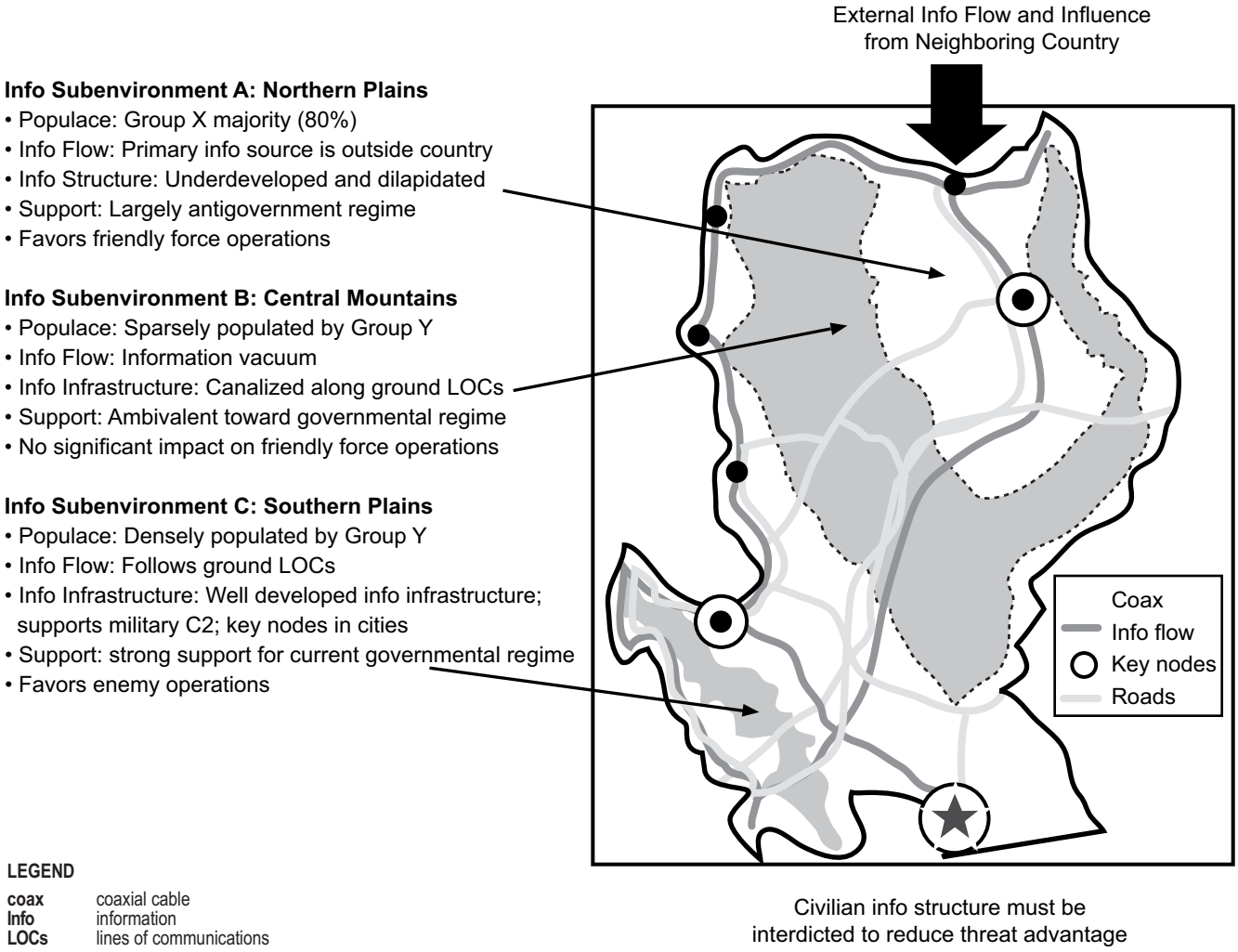
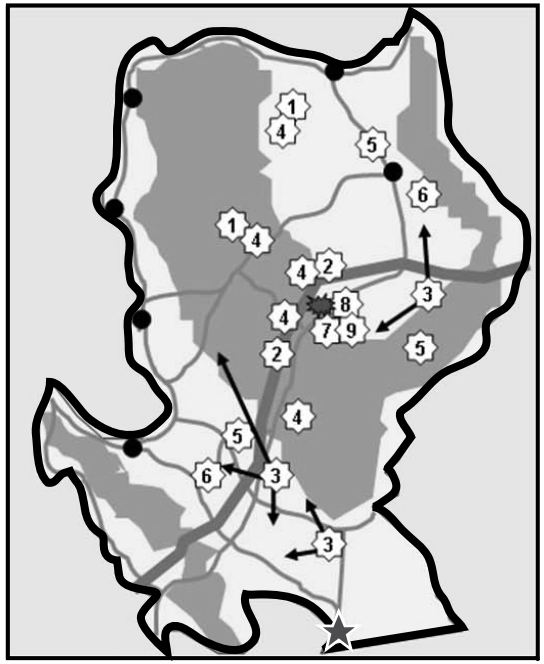


Figure B-2. Example of Combined Information Overlay.



Concept of Support: Short-word description of sequenced major elements in plan + definition of Info Superiority (IS) (resulting OP Advantage) . . .

IO Objectives:
1. Isolate
2. Disrupt
3. Influence

3-5 IO effects in the IE
- Task: Effect + Tgt (TA) + action/behavior
- Purpose: why

IO Essential Tasks:

KLE
1. Inform
2. Isolate

MISO
3. Isolate
4. Deny

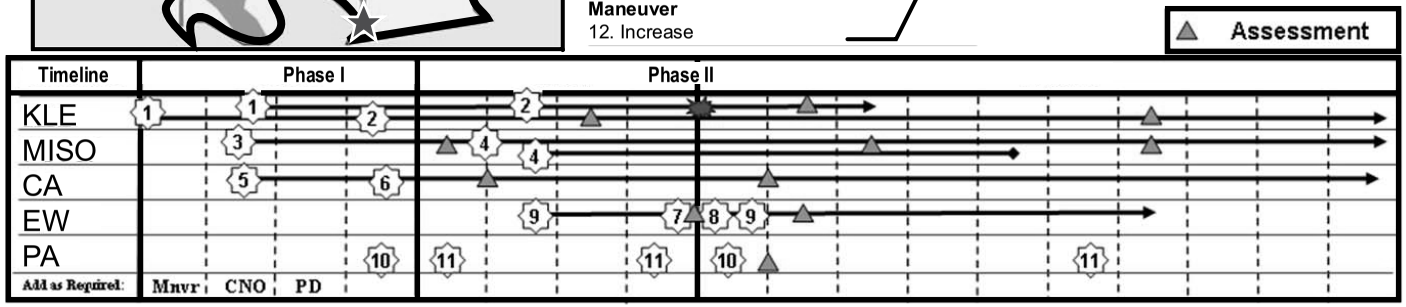
Civil Affairs
5. Increase local Upland Tribal support of . . .
6. Decrease IDP interface

EW
7. Degrade
8. Jam
9. Exploit

PA
10. Inform TA
11. Publicize adversary role

Maneuver
12. Increase

Essential IO actions required to achieve IS (the operational advantage):
- **Task:** Effect + Tgt (TA) + action/behavior
- **Purpose:** why
- **Method:** how
- **End state:** An essential IO task may support more than one IO objective.



LEGEND

IE	information environment	**OP**	operational
IDP	internal displaced persons	**PD**	public diplomacy
IO	information operations	**TA**	target audience
IS	information superiority	**Tgt**	target

Figure B-3. Example of an Information Operations Concept of Support Sketch.

APPENDIX C
SAMPLE OF APPENDIX 3 TO ANNEX C INFORMATION OPERATIONS

CLASSIFICATION

Copy no. ____ of ____ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time group
Message reference number

APPENDIX 3 (Information Operations) TO ANNEX C (Operations) TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) (U)
INFORMATION OPERATIONS (U)

(U) REFERENCES:

(a) Any relevant plans or orders.
(b) Required maps and charts.
(c) Other relevant documents.

1. (U) Situation. Summarize the overall operational situation as it relates to information operations.

a. (U) Adversary. Summarize the adversary situation, force disposition, intelligence capabilities, and possible courses of action. If applicable, reference intelligence estimates or summaries. Address any specific information that bears directly on the planned information operations.

b. (U) Friendly. Summarize the situation of those friendly forces that may directly affect attainment of information operations objectives. Address any critical limitations and any other planned information operations.

c. (U) Assumptions. List any assumptions made of friendly, adversary, or third party capabilities, limitations, or courses of action. Describe the conditions that the commander believes will exist at the time the plan becomes an order. Omit in orders.

2. (U) Mission. Provide the command's mission from the base order.

CLASSIFICATION

3. (U) Execution

a. (U) Concept of Support. Summarize how the commander visualizes the execution of information operations from its beginning to its termination. Describe how information operations will support the command's mission. Summarize the concepts for supervision and termination of information operations.

(1) (U) The concept of support may be a single paragraph or divided into two or more paragraphs depending upon the complexity of the operation.

(2) (U) When an operation involves various phases, such as peace or prehostilities or crisis, war, or post-hostilities, the concept of support should include subparagraphs describing the role of information operations in each phase.

b. (U) Information Operations Tasks. Identify the major tasks for each of the five elements of information operations. The five elements of information operations listed below are covered in tabs A through E.

(1) (U) Military deception.

(2) (U) Electronic warfare.

(3) (U) Operations security.

(4) (U) Military information support operations.

(5) (U) Physical attack.

c. (U) Coordinating Instructions. Address any mutual support issues relating to the elements of IO.

4. (U) Administration and Logistics. Address any IO administrative or logistic requirements.

5. (U) Command and Control. List any IO command and control instructions. State the command structure for information operations. Identify any special IO communications and reporting requirements.

CLASSIFICATION

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

TABS:

A – Military Deception
B – Electronic Warfare
C – Operations Security
D – Military Information Support Operations
E – Physical Attack

OFFICIAL:
s/
Name
Rank and Service
Title

This Page Intentionally Left Blank

GLOSSARY

SECTION I. ACRONYMS AND ABBREVIATIONS

BDA . . . . . battle damage assessment

C2 . . . . . command and control
CA . . . . . civil affairs
CAO . . . . . civil affairs operations
CCIR . . . . . commander's critical information requirement
CI . . . . . counterintelligence
CJCS . . . . . Chairman of the Joint Chiefs of Staff
CMO . . . . . civil-military operations
COA . . . . . course of action
COG . . . . . center of gravity
COMCAM . . . . . combat camera
COMSEC . . . . . communications security

DCO . . . . . defensive cyberspace operations
DISA . . . . . Defense Information Systems Agency
DOD . . . . . Department of Defense

EW . . . . . electronic warfare
EWCC . . . . . electronic warfare coordination cell
EWO . . . . . electronic warfare officer

FOps . . . . . future operations

G-1 . . . . . personnel staff section
G-2 . . . . . intelligence staff section
G-3 . . . . . operations staff section
G-6 . . . . . communications system staff section
G-9 . . . . . civil affairs staff section

HUMINT . . . . . human intelligence

IA . . . . . information assurance
IAM . . . . . information assurance manager
IAT . . . . . information assurance technician
INFOSEC . . . . . information security
IO . . . . . information operations
IOII . . . . . information operations intelligence integration
IOWG . . . . . information operations working group
IPB . . . . . intelligence preparation of the battlespace
IRC . . . . . information-related capability
ISR . . . . . intelligence, surveillance, and reconnaissance

J-3 . . . . . operations directorate of a joint staff
JCMA . . . . . Joint Communications Security Monitoring Activity
JMISTF . . . . . joint military information support task force
JP . . . . . joint publication
JTF . . . . . joint task force
JTF-GNO . . . . . Joint Task Force - Global Network Operations

MAGTF . . . . . Marine air-ground task force
MARCERT . . . . . Marine Corps Computer Emergency Response Team
MCEN . . . . . Marine Corps enterprise network
MCNOSC . . . . . Marine Corps Network Operations and Security Center
MCPP . . . . . Marine Corps Planning Process
MCRP . . . . . Marine Corps reference publication
MCWP . . . . . Marine Corps warfighting publication
MILDEC . . . . . military deception
MISG . . . . . military information support group
MISO . . . . . military information support operations
MOE . . . . . measure of effectiveness

NCIS . . . . . Naval Criminal Investigative Service

OCO . . . . . offensive cyberspace operations
OPORD . . . . . operation order
OPSEC . . . . . operations security
OPT . . . . . operational planning team
OPE . . . . . operational preparation of the environment

PA . . . . . public affairs
PAO . . . . . public affairs officer

RadBn . . . . . radio battalion

S-1 . . . . . personnel officer
S-2 . . . . . intelligence officer
S-3 . . . . . operations officer
S-6 . . . . . communications system officer
S-9 . . . . . civil affairs officer
SIGINT . . . . . signals intelligence
SJA . . . . . staff judge advocate
SME . . . . . subject matter expert
STO . . . . . special technical operations

US . . . . . United States

VMAQ . . . . . Marine tactical electronic warfare squadron

SECTION II. DEFINITIONS

area of operations—An operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. Also called **AO**. (JP 1-02)

branch—4. The contingency options built into the base plan used for changing the mission, orientation, or direction of movement of a force to aid success of the operation based on anticipated events, opportunities, or disruptions caused by enemy actions and reactions. See also **sequel**. (JP 1-02, part 4 of a 4 part definition)

center of gravity—The source of power that provides moral or physical strength, freedom of action, or will to act. Also called **COG**. See also **decisive point**. (JP 1-02)

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

civil affairs operations—Those military operations conducted by civil affairs forces that (1) enhance the relationship between military forces and civil authorities in localities where military forces are present; (2) require coordination with other interagency organizations, intergovernmental organizations, nongovernmental organizations, indigenous populations and institutions, and the private sector; and (3) involve application of functional specialty skills that normally are the responsibility of civil government to enhance the conduct of civil-military operations. Also called **CAO**. See also **civil affairs; civil-military operations**. (JP 1-02)

civil information management—The process whereby civil information is collected, consolidated in a central database, and shared with the supported elements, higher headquarters, other US Government and Department of Defense agencies, international organizations, and nongovernmental organizations. (This term and its definition are proposed for inclusion in the next edition of MCRP 5-12C.)

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)

combat camera—The acquisition and utilization of still and motion imagery in support of operational and planning requirements across the range of military operations and during exercises. Also called **COMCAM**. (MCRP 5-12C)

communications security—The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (JP 1-02)

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

counterintelligence—Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. Also called **CI**. (JP 1-02)

cyberspace intelligence, surveillance, and reconnaissance—An intelligence action conducted by the joint force commander authorized by an executive order or conducted by attached signals intelligence units under temporary delegated signals intelligence operational tasking authority.

cyberspace operational preparation of the environment—Consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations.

cyberspace operations—The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 1-02)

decisive point—A geographic place, specific key event, critical factor, or function that, when acted upon, allows commanders to gain a marked advantage over an adversary or contribute materially to achieving success. See also **center of gravity**. (JP 1-02)

defensive cyberspace operations—Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called **DCO.** (JP 1-02)

demonstration—2. In military deception, a show of force in an area where a decision is not sought that is made to deceive an adversary. It is similar to a feint but no actual contact with the adversary is intended. (JP 1-02 part 2 of a 2 part definition)

Department of Defense information network operations—Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 1-02)

display—In military deception, a static portrayal of an activity, force, or equipment intended to deceive the adversary's visual observation. (JP 1-02)

electronic attack—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**. See also **electronic protection; electronic warfare; electronic warfare support**. (JP 1-02)

electronic protection—Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Also called **EP**. See also **electronic attack, electronic warfare; electronic warfare support**. (JP 1-02)

electronic warfare—Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. (JP 1-02)

electronic warfare support—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.

Also called **ES**. See also **electronic attack; electronic protection; electronic warfare**. (JP 1-02)

feint—In military deception, an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action. (JP 1-02)

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

information environment—The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02)

information operations—The integration, coordination, and synchronization of all actions taken in the information environment to affect a target audience's behavior in order to create an operational advantage for the commander. Also called **IO** (This term and its definition are proposed for inclusion in the next edition of MCRP 5-12C)

information operations intelligence integration—The integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities, determine effects, and assess the information environment. Also called **IOII**. (JP 1-02)

information-related capability—A capability, function, or activity that uses data, information, or electromagnetic spectrum to produce lethal or nonlethal effects in the physical or informational dimensions with an expressed intent to cause deliberate effects within the cognitive dimension of the information environment. Also called **IRC**. (Proposed for inclusion in the next edition of MCRP 5-12C)

information superiority—The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also **information operations**. (JP 1-02)

measure of effectiveness—A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. Also called **MOE**. (JP 1-02)

measure of performance—A criterion used to assess friendly actions that is tied to measuring task accomplishment. Also called **MOP**. (JP 1-02)

military deception—Actions executed to deliberately mislead adversary, paramilitary, or violent extremist organization military decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Also called **MILDEC**. (JP 1-02)

military information support 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 in a manner favorable to the originator's objectives. Also called **MISO**. (JP 1-02)

offensive cyberspace operations—Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called **OCO**. (JP 1-02)

operations security—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. Also called **OPSEC**. (JP 1-02)

physical attack—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. (This term and its definition are proposed for inclusion in the next edition of MCRP 5-12C)

physical security—1. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02, part 1 of a 2 part definition)

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

public affairs guidance—Constraints and restraints established by proper authority regarding public information, command information, and community relations activities. It may also address the method(s), timing, location, and other details governing the release of information to the public. Also called **PAG**. See also **public affairs**. (JP 1-02)

public diplomacy—1. Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. 2. In peace building, civilian agency efforts to promote an understanding of the reconstruction efforts, rule of law, and civic responsibility through public affairs and international public diplomacy operations. (JP 1-02)

ruse—In military deception, a trick of war designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system. (JP 1-02)

security cooperation—All Department of Defense interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation. Also called **SC**. (JP 1-02)

sequel—The subsequent major operation or phase based on the possible outcomes (success, stalemate, or defeat) of the current major operation or phase. See also **branch**. (JP 1-02)

staff judge advocate—A judge advocate so designated in the Army, Air Force, or Marine Corps, and the principal legal advisor of a Navy, Coast Guard, or joint force command who is a judge advocate. Also called **SJA**. (JP 1-02)

target—1. An entity or object considered for possible engagement or other action. 2. In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. 3. An area designated and numbered for future firing. 4. In gunfire support usage, an impact burst that hits the target. (JP 1-02)

target audience—An individual or group selected for influence. Also called **TA**. (JP 1-02)

REFERENCES AND RELATED PUBLICATIONS

Federal Publications

Executive Order

12333	United States Intelligence Activities

United States Code

Title 10	Armed Forces

Department of Defense Issuances

Department of Defense Directives (DODDs)

S-3600.1	Information Operations
8570.01	Information Assurance (IA) Training, Certification, and Workforce Management

Department of Defense Instruction (DODI)

8510.01	DOD Information Assurance Certification and Accreditation Process (DIACAP)

Joint Publications (JPs)

1-02	Department of Defense Dictionary of Military and Associated Terms
2-01.3	Joint Intelligence Preparation of the Operational Environment
3-13	Information Operations
3-13.1	Electronic Warfare
3-13.2	Military Information Support Operations
3-13.3	Operations Security
3-13.4	Military Deception
3-57	Civil-Military Operations
3-61	Public Affairs
6-0	Joint Communications System

Marine Corps Publications

Marine Corps Warfighting Publications (MCWPs)

2-1	Intelligence Operations
2-6	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
3-33.7	MAGTF Combat Camera
3-40.2	Information Management
3-40.3	MAGTF Communications System
3-40.5	Electronic Warfare
3-40.6	Psychological Operations

3-40.9 Operations Security (OPSEC)
5-1 Marine Corps Planning Process

Marine Corps Reference Publications (MCRPs)
2-3A Intelligence Preparation of the Battlefield/Battlespace
3-33.7A Multi-Service Tactics, Techniques, and Procedures for Combat Camera Operations
3-40.4A Multi-Service Tactics, Techniques, and Procedures for Military Deception (MILDEC) Operations (classified)
5-12C Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms

Marine Corps Orders (MCOs)
3070.2 The Marine Corps Operations Security (OPSEC) Program
3104.1_ Marine Corps Combat Camera Program
3120.10 Marine Corps Information Operations Program

Miscellaneous
Marine Corps Operating Concept for Information Operations

Miscellaneous

Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*