MCWP 3-36

Information Operations

U.S. Marine Corps

Coordinating Draft 2-27-01

PCN XXX XXXXXX XX

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-0001

DATE

FOREWORD

1. PURPOSE

Marine Corps Warfighting Publication (MCWP) 3-36, *Information Operations,* introduces doctrine for employment and use information operations (IO) in support of the Marine Air-Ground Task Force (MAGTF) operations.

2. SCOPE

This manual is intended to provide an introduction to information operations and a specific foundation in information warfare planning for Marines. Because Marines are primarily warfighters, this manual necessarily emphasizes those concepts key to operational planning for conflict. It provides a basis for Marines to understand the relevance of information operations and a planning framework for the implementation of information operations.

The language and organization of information operation concepts continue to evolve and to be debated at the highest levels. This publication gives Marines a warfighter’s orientation to information operations and its use to resolve conflicts now. It is first and foremost an implementation guide.

This manual provides an overview of information operation elements, planning processes, and tasks for MAGTF information operations. It is not intended exclusively for personnel who work within the field of information operations.

3. SUPERSESSION

None.

4. CERTIFICATION

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

B.B. KNUTSON JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command
Quantico, Virginia

MCWP 3-36
Information Operations

TABLE OF CONTENTS

CHAPTER 1
FOUNDATIONS OF IO

Introduction. Marines play a vital role in the defense of our nation's national interests. In fulfilling their role Marines act to support our nation's strategy through engagement during peace and by ensuring victory during conflict. As our nation's force in readiness Marines will confront many new changes and must be prepared to provide the success that our nation expects. This means that Marines must use all their combat capabilities to the best advantage. These capabilities include the control and the use of information.

A Changing World. The world is going through dynamic changes that will change the operational environment in which Marine forces will deploy and fight in the future. These changes have been brought about by many factors. The rapid advance of technology; the emergence of new adversaries; and the Marine Corps' increasing involvement in humanitarian and peace support missions are all contributing to a new, and increasingly complex, operational environment.

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

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

New Adversaries. Marines face a range of traditional and non-traditional threats. Many countries still have the capability to threaten U.S. interests abroad and can initiate a major conflict that would require a large-scale U.S. response. However, many other lesser threats exist across the range of operations that fall short of war. Terrorists, drug cartels, computer hacker groups, as well as rogue nations, who might act independently in their own self-interest, are some examples. Using new technology and information these threats have the capability to threaten the U.S. across geographic borders through networks. They may avoid direct military confrontation and attack selected vulnerabilities in order to achieve a high payoff for little cost or for the media exposure it brings.

New Missions. The U.S. recognizes a wide range of domestic and global security and humanitarian responsibilities. Marines may be asked to provide humanitarian assistance after a disaster, provide peace support for nations that seek a secure environment to peacefully develop, provide peace enforcement to separate warring factions and create

conditions for the peaceful resolution of a crisis, and finally to project combat power when resolving a crisis requires the use of force. As a crisis develops, Marines may find themselves executing more than one mission at a time. They may be asked to provide relief to civilians while keeping belligerents separated, defending U.S. interests, and enforcing international law.

Expeditionary Operations. An expedition is a military operation conducted by an armed force to accomplish a specific objective in a foreign country. The missions of military expeditions vary widely. Examples of missions of military expeditions include providing humanitarian assistance in times of disaster or disruption; establishing and keeping the peace in a foreign country; protecting U.S. citizens or commerce abroad; retaliating for an act of aggression by a foreign political group; thwarting trans-national terrorist and criminal threats; and protecting U.S. interests by defeating enemy armed forces in combat.

Expeditionary operations occur across the continuum of peace, crisis, and war. And, the defining characteristic of expeditionary operations is the projection of force into a foreign setting. The 21st century security environment will confront the United States with situations of vast political and military complexity and geographic dispersion. To meet these challenges the Marine Corps must maintain a force with a full-spectrum of capabilities to deter conflicts, to respond to crisis, and to fight and win against any foe.

IO is inherently suited to expeditionary operations due to its lethal and non-lethal aspects, its ability to project force or influence, and its ability to provide a tailored response to a specific mission or crisis environment. Finally, IO operations are scalable. They can increase or decrease in intensity as required to support emerging circumstances. Scalability to enable crisis management, the ability to conduct economy of force operations, and the ability to project force and/or influence as the situation dictates, all these aspects of IO reinforce the Marine Corps' ability to project and sustain decisive military power in forward areas.

Fundamentals.

The following fundamentals are essential to successfully understanding the potential that IO possesses to help the MAGTF achieve operational success.

- *MAGTF IO is different*. Marines organize as MAGTFs. The ability to integrate combat power in order to win in conflict is inherent in Marine Corps organization and the expeditionary mindset of the individual Marine. Marines intuitively understand task-organization. Integration of capabilities is a part of how Marines fight.

- *MAGTF IO is focused on the objective.* Like all operations, Information Operations ultimately exists to help the MAGTF achieve its mission. A thoughtful analysis of the MAGTF mission and a subsequent strategy-to-task analysis of IO activities are

essential. No activity exists independent of the compelling requirement for the MAGTF to meets its objective. A carefully structured IO plan preserves MAGTF resources and may greatly assist the MAGTF in synchronizing the activities of a wide variety of agencies with those of the MAGTF.

- *The MAGTF commander's intent and concept of operations determine IO targets and objectives.* The MAGTF should determine the vulnerabilities and critical elements of friendly and enemy information, information-based processes, and information systems. Those key elements, the destruction or degradation of which would support the accomplishment of the unit mission, should be targeted appropriately. MAGTF command and control systems are a substantial target for adversary IO. Systems critical to the friendly forces should be protected. Control, coordination, and management of influences such as media, messages, and personal contact should be exercised to the advantage of the MAGTF.

- *MAGTF IO must be synchronized and integrated with those of the higher and adjacent commands.* Information Operations will be conducted in battlespace that has already been shaped by Commanders-in-Chief (CINCs) peacetime regional and theater engagement activities. During joint operations, the joint force commander (JFC) provides guidance and direction for conducting IO to support his mission, concept of operations, objectives, and intent. The MAGTF IO plan, while leveraging and exploiting the IO capabilities of higher echelons in support of the MAGTF, must also support the JFC's IO objectives to achieve unity of effort and avoid undermining the JFC IO plan.

- *Many different capabilities and activities must be integrated to achieve a coherent IO strategy.* The support of the warfighting functions of the MAGTF (maneuver, fires, logistics, force protection, intelligence, and C2), as well as the design and operation of information systems is critical to the successful conduct of IO.

- *Intelligence support is critical to the planning, execution, and assessment of IO.* IO requires accurate, timely, and detailed intelligence, to include intelligence preparation of the battlespace (IPB) products. Intelligence analysis should determine the enemy's potential IO vulnerabilities and capabilities. Analysis may also help in defining suitable measures of effectiveness. An early assessment of key enemy centers of gravity is essential.

The MAGTF should fully integrate the planning and execution of IO into its concept of operations in order to maximize the effects of its actions on the enemy. IO is a complex endeavor involving many units and agencies, both organic and supporting to the MAGTF. To be successful, the offensive and defensive aspects of IO, intelligence, and other information-related activities that provide information on friendly and enemy forces, and friendly information systems (to include the friendly decision-making process) must be integrated. These activities require detailed planning and coordination with a single unifying purpose.

This sole purpose, the goal of IO, is to support the commander's intent and facilitate accomplishment of the MAGTF mission. IO attacks (or protects) information and information systems and degrades the quality of the adversary's decision-making. IO can slow or halt entirely the flow of information; it can change the accuracy or useability of the data within the information system. The decision-making process is dependent upon information. Poor information prevents the enemy from developing accurate situation awareness and slows down his decision-making process

Information Operations. Information Operations (IO) includes all actions taken to affect enemy information and information systems while defending friendly information and information systems. IO is conducted during all phases of an operation, across the range of military operations, and at every level of war. In some environments IO capitalizes on the growing sophistication, connectivity, and reliance on information technology and focuses on the vulnerabilities and opportunities presented by the increasing dependence of the U.S. and its adversaries on information and information systems.

In other situations, IO may mean employing decidedly low-tech means, such as exploiting cultural factors or less sophisticated means of communication, to facilitate civil-military operations (CMO), psychological operations (PSYOP), or tactical deception. Whatever the nature of the conflict, IO targets information or information systems to affect the information-based decision-making process. IO may, in fact, have its greatest impact as a deterrent in peace and during the initial stages of crisis. IO may help deter adversaries from initiating actions detrimental to the U.S.. At every echelon of command and all levels of warfare, some form of IO is likely to be a critical tool in achieving the objectives of the commander.

Information Operations Categories.

There are two mutually supporting categories of IO. IO conducted during conflict is referred to as IW. See figure X.

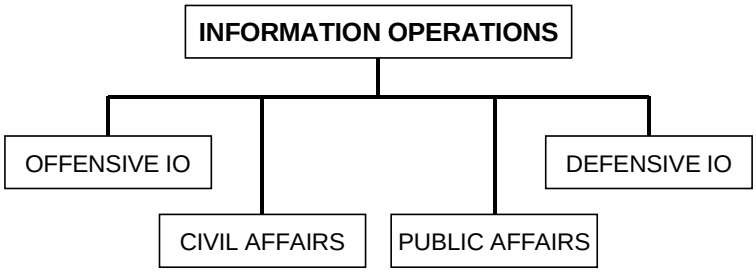

Figure X. Information Operations categories.

Offensive Information Operations. Offensive IO involves the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision-makers and their information and information systems. These capabilities and activities include, but are not limited to: operations security (OPSEC), military deception, PSYOP, electronic warfare (EW), physical attack/destruction, and computer network operations (CNO). The human decision-making

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

During conflict, when employed as an integrating strategy, IW weaves together related offensive IO capabilities and activities toward satisfying a stated objective. Offensive IO influences enemy information by PSYOP, OPSEC, and military deception, and degrades the flow of information by EW and physical attack and destruction. The integrated use of these methods can disrupt the enemy decision-making process. See figure X.

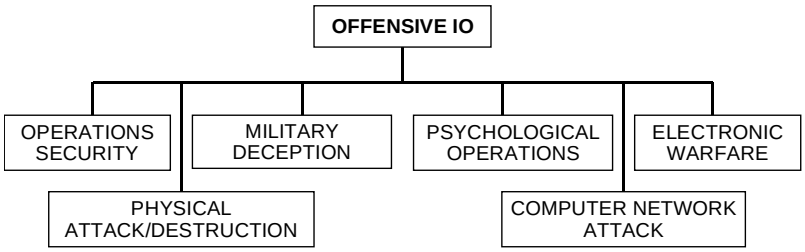

Figure X. Elements of Offensive Information Operations.

Offensive IO Planning. During planning, it is essential that IO planners consider the adversary's C2 as a system that is made up of personnel, equipment, information, and procedures that work together to allow the adversary commander to accomplish his mission. Also, a product of the adversary C2 system is the adversary's perceptions, decisions, and reactions. Thus, offensive IO targets adversary C2 systems (e.g. radars, communication nodes, information systems) as well as the decision-maker and his decision cycle (e.g. the mind of the enemy commander, command nodes, intelligence systems). Offensive IO is exercised through the overall IO plan and an effective offensive IO plan. Its foundation is a clear understanding of the friendly mission and a thorough analysis of the enemy C2 system (including biases and decision-making processes). The analysis of enemy's C2 system to determine critical and vulnerable nodes is called *nodal analysis*.

Goals of offensive IO include:

- Slow the adversary's tempo of operations.
- Disrupt the adversary's operations and plans.
- Disrupt the adversary commander's ability to generate combat power.
- Degrade the adversary commander's decision cycle for executing mission orders and movement instructions.

Potential results of offensive IO include:

- Slow the adversary's operational tempo.

- Disrupt adversary plans. Disrupt the adversary commander's ability to focus combat power.
- Influence the adversary commander's estimate of the situation.

Defensive Information Operations. Defensive IO integrates and coordinates policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive IO is conducted and assisted through information assurance, OPSEC, physical security, counter-deception, counterpropaganda, counterintelligence (CI), and EW. During operational planning an analysis of friendly information systems and their vulnerabilities (nodal analysis) is conducted with a risk assessment in order to determine defensive IO measures and priorities.

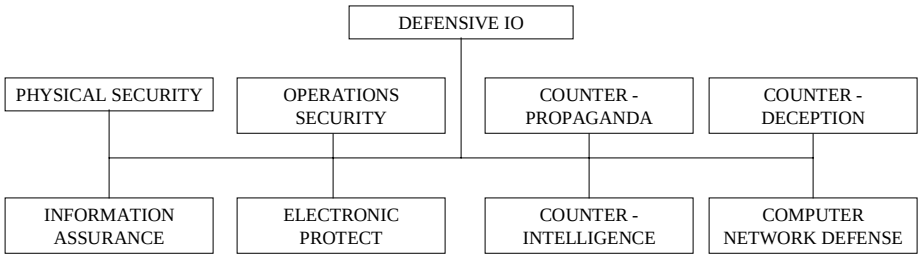

Figure X. Elements of Defensive Information Operations.

Defensive IO ensures timely, accurate, and relevant information access while denying the enemy the opportunity to exploit friendly information and information systems for their own purposes. Since it is a practical impossibility to defend every aspect of the infrastructure and every information process, defensive IO provides the essential and necessary protection and defense of information and information systems upon which the MAGTF depends to conduct operations and achieve objectives. A useful guide is CJCSI 6510.01B *Defensive IO Implementation*. Four interrelated processes comprise defensive IO:

- Information Environment Protection. Defining MAGTF needs, risks, vulnerabilities is the focus of information environment protection. The protected information environment is a combination of information systems and facilities, as well as abstract processes such as intelligence collection and analysis. The MAGTF

should establish a protected information environment through development of common policies, procedures, incorporation of appropriate technological capabilities, and a strong focus on operational support.

- Attack Detection. Determination and identification of enemy capabilities (such as EW and military deception) and their potential to affect friendly information and information systems, timely detection of such attacks, and immediate reporting are the keys to the restoration of degraded system capabilities and development of a response to the attack.

- Capability Restoration. Capability restoration relies on established procedures and mechanisms for the prioritized restoration of essential information and information system functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer. Information system design should incorporate automated restoration capabilities and other redundancy options. A post-attack analysis should be conducted to determine the command vulnerabilities and recommended security improvements.

- Attack Response. IO attack detection or validation of a potential attack through analysis should trigger the command response. Timely identification of the attackers and their intent is the cornerstone of effective and properly focused response, thereby linking the analytic results of the intelligence process to appropriate decisionmakers. The response contributes to defensive IO by countering future threats and enhancing deterrence. Although attack response can include diplomatic, legal, or economic actions, the MAGTF will normally focus on military force. These options include the range of lethal and nonlethal responses that may eliminate the threat directly or interrupt the means or systems that the enemy used to conduct the IO attack.

Defensive IO Planning. Defensive IO plans are developed to ensure effective friendly use of the electro-magnetic spectrum while negating adversary efforts to do the same. Defensive IO reduces friendly C2 vulnerabilities to adversary attack by employment of adequate physical, communications, electronic, and operations security measures. Additionally, on-going coordination and de-confliction is required to reduce friendly mutual interference and manage the electro-magnetic spectrum is support of friendly command and control.

The basis for defensive IO planning is the conduct of operations security surveys, C4 vulnerability analysis, identification of essential elements of friendly information (EEFIs), and the generation of the restricted frequency list (RFL).

Goals of defensive IO include:

- Reduce the adversary’s ability to effect friendly C2, primarily through defensive measures
- Reduce friendly mutual interference in C2 throughout the electromagnetic spectrum

Potential results of defensive IO include:

- Minimize friendly C2 system vulnerabilities to adversary C2-attack through the employment of adequate physical, electronic, information, and operations security measures.
- Minimize friendly mutual interference on friendly C2 and unintended third parties.

Other Related Activities. Related activities are operations that are neither offensive nor defensive in nature but must be coordinated with all other IO efforts. Such activities include public affairs (PA) and civil-military operations (CMO). PA and CMO (supported by civil affairs units) are pervasive and continuous. MAGTFs may find PA and civil military activities on-going within their operational area as part of an international, national or CINC engagement or battlespace shaping initiative. These activities will influence tactical IO/IW initiatives.

Intelligence Support.

Intelligence support is critical to the planning, execution, and assessment of IO. IO can be a voracious consumer of intelligence and may require dedicated intelligence resources and assets.

Many IO intelligence requirements require significant lead-time to develop collection sources, access, and databases. Potential intelligence collection sources should be developed as early as possible. Potential sources include national and theater-level human intelligence (HUMINT) and SIGINT operations, as well as open source materials (such as the internet, commercial publications and radio/television).

IO will require development of extensive intelligence analytical products in order to obtain a detailed knowledge of the enemy use of information and information systems. Intelligence analysis to support both offensive IO and defensive IO will require the following information:

- Technical requirements of a wide array of information systems.
- Enemy C2 systems, to include nodal analyses, electronic order of battle, communication patterns, operating frequencies, and electronic IPB templates.
- Enemy doctrine and tactics.
- Political, economic, social, cultural and personal influences on decision-makers.
- An understanding of the enemy’s decision-making process.
- Knowledge of the biographical background of key enemy decision-makers and their advisors, to include biographical sketches, career histories, motivating factors, and leadership styles.
- Geographic and atmospheric influence on enemy and friendly communications.
- Assessment of potential enemy capability and intent to attack or exploit friendly information and information systems.

The role of intelligence is continual. Changes in enemy information systems and operating patterns must be detected, analyzed, and reported

to ensure that IO continues to attack the correct targets. Assessment of ongoing IO activities is a crucial, and extremely challenging, responsibility of intelligence. Targets must be monitored to determine the effectiveness of the IO efforts. To achieve complete synthesis, IO must be incorporated into the MAGTF's Intelligence, BDA, and Targeting cycles. The impact of many IO actions may be difficult to measure, and indicators of success or failure must be carefully crafted in advance. Once detected, these indicators should be reported immediately to IO planners so that appropriate action can be taken.

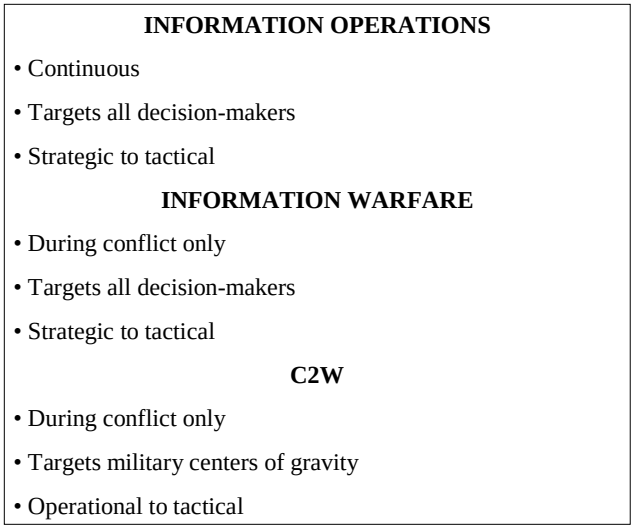

Figure X. IO, IW, and C2W Relationship.

Information Operations and the Levels of War.

Although IO is conducted at all levels of war, the purpose and target of IO may differ at each level. The boundaries between these levels may not be distinct and IO actions at one level of war may impact other levels.

Strategic Level of War. IO may be included in the spectrum of activities directed by the National Command Authorities to achieve national objectives by influencing or affecting all elements (political, military, economic, or informational) of an enemy's or potential enemy's national power while protecting similar friendly elements. There should be a high degree of coordination between the military, other U.S. Government departments and agencies, and allies or coalition partners to achieve these objectives.

Operational Level of War. At this level, IO is conducted to achieve or support campaign or grand tactical objectives. The focus of IO at this level is to affect enemy communications, lsupport, command and control, and related capabilities and activities while protecting similar friendly capabilities and activities. Operational level IO may contribute to achieving strategic objectives by degrading an enemy's capability to organize, command, deploy, and sustain military forces

and capabilities and by allowing Marine forces to obtain and maintain the degree of information superiority required to quickly and decisively accomplish its mission.

Tactical Level of War. IO, called IW during conflict, at this level facilitates achieving specific tactical objectives. The primary focus of IO is to affect enemy information and information systems relating to C2, intelligence, and other information-based processes directly relating to the conduct of military operations while protecting similar friendly capabilities.

Information Operations and the MAGTF.

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

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

Information Operations and the Marine Corps Component.

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

The Marine Corps component commander accomplishes the assigned mission by conducting Marine Corps component operations. With respect to IO, the Marine Corps component commander focuses on those activities that will support future operations — the next Marine Corps component mission — and coordinates IO actions with other component commanders to

achieve unity of effort for the joint force. The IO orientation of the Marine Corps component commander is *normally* at the operational level of war while the MAGTF commander is *normally* at the tactical level. Naturally, there will be some overlap.

The Marine Corps component provide IO support to the MAGTF by:

- Planning access to national, theater, and joint task force intelligence system architectures and databases in conjunction with the component intelligence staff.
- Developing component IO policy as needed consistent with the JFC's IO policies.
- Ensuring that the capabilities of the Marine Corps are integrated in the operations plans, contingency plans and future plans of the CINC.
- Representing Marine forces in the joint force IO cell and at joint boards as required (e.g., for targeting and intelligence collection) in order to set conditions favorable to the MAGTF's mission accomplishment.

For more information regarding component responsibilities, see MCWP 0-1.1, *Componency*.

CHAPTER 2
IO OPERATIONAL PLANNING

Thorough planning is the key to the successful implementation of IO. MAGTF planners must ensure that IO planning begins at the earliest stage of operation planning, is nested within the IO plans of the higher headquarters, and fully integrated into the unit operation plan. The IO cell and the Marine Corps Planning Process (MCPP) are two important tools in successful IO planning.

The Information Operations Cell.

The IO cell is a task-organized group of individuals brought together within a MAGTF and higher headquarters to focus a variety of separate disciplines and functions on IO for the command. A fully functioning IO cell integrates a broad range of potential IO actions and related activities that contribute to accomplishing the mission. Ensuring that IO is an integral part of all operations requires extensive planning and coordination among all the elements of the staff. The IO cell is the mechanism for achieving that coordination.

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

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

Responsibilities for IO

The G-3 is responsible for IO. The Future Operations Section is responsible for overseeing the planning and coordination of the IO effort.

The MAGTF IO Officer, within G-3 Future Operations, is responsible for the broad integration and synchronization of IO efforts. He is responsible directly to the G-3 for MAGTF IO. He ensures that the IO Cell provides input to the Operations Planning Team during planning to ensure coordinated operations. The MAGTF IO Officer oversees the core personnel within the IO Cell and calls additional IO Cell meeting as required to augmentees from external agencies. He ensures that all IO matters are coordinated within the MAGTF staff, with higher headquarters, and with external agencies.

The Electronic Warfare Officer (EWO) integrates electronic warfare (EW) operations through the EW Coordination Center (EWCC).

The G-2 disseminates intelligence required to implement the IO strategy to include assessments on enemy tactics, techniques, equipment, order of battle, and the intelligence aspects of EW and deception.

The Fire Support Coordinator (FSC), Supporting Arms Coordinator (SAC), Target Information Officer (TIO), and Target Intel Officer together oversee the formation of the target list and the engagement of those targets.

The G-6 oversees the communications security program, supports the installation and maintenance of information systems, assists the EWO in de-conflicting EW jamming operations, and assists in prioritization of the defensive information operations effort.

The Signals Intelligence Officer (SIO) oversees attached signals intelligence (SIGINT) assets, maintains liaison with the Joint Intelligence Center (JIC), and oversees processing and sanitization of reports containing special intelligence (SI).

The Marine Corps Planning Process.

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

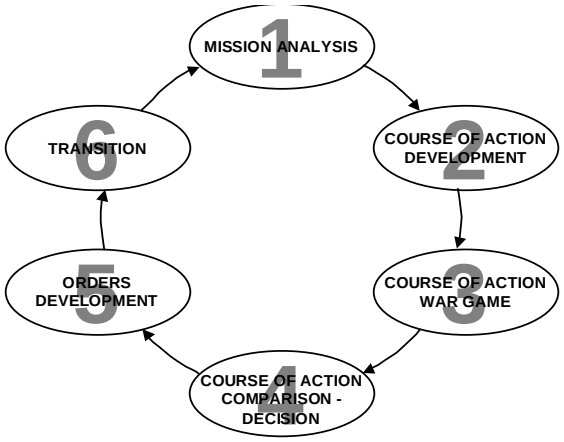

Figure 2-1. Marine Corps Planning Process steps.

The MCPP organizes the planning process into six manageable, logical steps (see figure 2-1). It establishes procedures for analyzing a mission, developing and wargaming COAs against the threat, comparing friendly COAs against the commander's criteria and each other, selecting a COA, and preparing an operation order for execution. It

provides the commander and his staff a means to organize their planning activities and transmit the plan to subordinates and subordinate commands. IO planning is aligned with the MCPP steps and ensures IO actions are coordinated with all six warfighting functions and the operations of higher, adjacent, and subordinate commands.

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

Mission Analysis.

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

The higher headquarters order is analyzed to extract IO planning guidance such as constraints, restrictions, 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 mission analysis, IPB planning supports the commander as he develops his battlespace area evaluation. Assisted by the intelligence section, the MAGTF IO cell reviews known facts about the enemy C2 status and the host-nation environment. IPB products relevant to further IO planning are developed or requested. Enemy centers of gravity are determined. Potential risks and friendly vulnerabilities are also identified for defensive IO actions. Information gaps must be determined and requests submitted to resolve the uncertainties necessary for further planning. Unique IO factors, such as IO ROE and assumptions, are identified during mission analysis. IO planners conduct a strategy to task analysis that links the MAGTF mission to strategic and operational IO objectives.

An initial concept for IO support can be developed during this step. Friendly IO assets and capabilities, either organic or supporting the MAGTF as well as additional IO force structure requirements, are identified. Desired results can be determined. The IO concept of support must be focused by and in accordance with the commander’s initial guidance. A staff estimate for IO is the most formal form of this concept of support and should be considered.

As mission analysis is conducted, resource or capability shortfalls are noted. The IO Cell should identify critical shortfalls and request support from higher headquarters or external agencies.

The IO cell must participate in the MAGTF’s planning activities and constantly coordinate its planning efforts with those of the MAGTF future operations section. Future operations will usually form an ad

hoc organization known as the operational planning team (OPT). The OPT will be doing its own mission analysis, and results of each group's (OPT and IO Cell) analysis will be valuable to the other. The friendly vulnerabilities can be incorporated into force protection planning, while the enemy critical vulnerabilities determined through the OPT's center of gravity analysis (COG) 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 campaign.

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

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

Course of Action Development.

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

Planning started during mission analysis will continue in COA development. The IPB products developed or requested will be reviewed for applicability with the commander's planning guidance. As necessary, IPB products will be modified and updated. As new information is received, CCIRs may be revised and additional requirements submitted. IO cell planning efforts will continue to be closely linked with those of the OPT. To assist the OPT, the IO cell may graphically display friendly IO assets and enemy C2 links and nodes to allow the planners to see the current and projected capabilities of friendly and enemy forces. Enemy IO strengths and vulnerabilities are identified through detailed nodal analysis for additional examination and possible exploitation. In coordination with the Red Cell and the G-2, the IO cell will develop an assessment of relative IO capabilities to provide the OPT with an understanding of the strengths and weaknesses of both friendly and enemy forces. The IO cell will conduct an assessment of friendly vulnerabilities to enemy IO actions. The IO cell will also continue to refine its analysis of the enemy COG to determine the critical enemy vulnerabilities most susceptible to IO. The refined COGs and critical vulnerabilities are used in the development of the initial COAs.

The IO cell will closely follow the development of the OPT COAs to ensure that the IO concept of support adequately supports these COAs. The IO cell may formulate an IO concept of support that will identify

those 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 that addresses the unique IO support requirements of each. 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 are to be accomplished?
- Who (IO assets) will execute the tasks?
- When are the IO tasks to occur?
- Where are the IO tasks to occur?
- Why is each IO task required?
- How will the MAGTF employ the IO capabilities to accomplish the tasks, and how is the IO concept nested with the higher headquarters IO plan? (An initial IO synchronization matrix can be developed to describe the answers to the above questions. Such a product will be useful in the following step of the MCPP.)

At the conclusion of COA development, the IO cell may have developed an overall IO concept, an IO concept of support for each COA, recommendations for the commander's wargaming guidance and evaluation criteria, updated IO associated IPB products, input to the COA graphic and narrative, and an initial staff estimate for IO with additional asset requirements identified as appropriate.

Course of Action War Game.

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

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

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

- Updated IPB products.
- Refined staff estimate for IO.
- Refined CCIRs.

- Task organization and asset shortfalls for IO resources.
- IO input to COA synchronization matrix.

Course of Action Comparison and Decision.

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

As appropriate, the IO cell may provide additional comparison criteria directly relevant to IO that may assist the commander in his decision. The IO results from the COA war game may be briefed as a separate, supporting concept by the IO cell, or presented by the OPT as an element of the overall plan. In any event, the IO cell is responsible for ensuring that the impact and anticipated effect of IO actions upon the enemy for each COA, and the relative merit of each COA from an IO perspective are provided to the commander.

Orders Development.

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

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

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

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

Because IO is multi-disciplined, it is found in various portions of the MAGTF Operations Order. [See below and CJCSM 3122.03*(Joint Operational Planning and Execution System Volume II, Planning Formats and Guidance)*.] The elements of IO are included as Tabs to the Appendix 3 (IW) to the OPORD. However, related areas include intelligence, communications, public affairs, and civil affairs. See Annex X of this publication for sample OPORD formats.

APPENDIX 2 (SIGNALS INTELLIGENCE) TO ANNEX B (INTELLIGENCE)

APPENDIX 4 (TARGETING) TO ANNEX B (INTELLIGENCE)

APPENDIX 6 (INTELLIGENCE SUPPORT TO C2W) TO ANNEX B (INTELLIGENCE)

APPENDIX 3 (INFORMATION WARFARE) TO ANNEX C (OPERATIONS)
TAB A – MILITARY DECEPTION
TAB B – ELECTRONIC WARFARE
TAB C – OPERATIONS SECURITY
TAB D – PSYCHOLOGICAL OPERATIONS
TAB E – PHYSICAL DESTRUCTION
TAB F – COMPUTER NETWORK ATTACK
TAB G – DEFENSIVE INFORMATION OPERATIONS

APPENDIX 1 (INFORMATION ASSURANCE) TO ANNEX K (COMMAND, CONTROL, AND COMMUNICATION, AND COMPUTER SYSTEMS)

ANNEX F (PUBLIC AFFAIRS)

ANNEX G (CIVIL AFFAIRS)

ANNEX S (SPECIAL TECHNICAL OPERATIONS)

ANNEX U (INFORMATION MANAGEMENT)

Transition.

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

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

IO Planning Model

IO planning falls within the normal planning a MAGTF Staff would perform for any mission. The main function of the MCPP is to develop courses of action. IO planning naturally focuses on the IO course of action within the overall planning process.

It is helpful to understand specifically how IO planning may accomplished. To do this, it is useful to build an IO Planning Process that breaks IO planning into further steps. The following model is not intended to dictate planning procedures to MAGTFs, rather, it is an illustration that allows Marine planners to begin to operationalize IO

concepts. Also, it is important to note that these steps occur within the MCPP framework. They are simply a subset of IO planning procedures and each supports a MCPP planning step.

IO, called IW during conflict, is a combination of both offensive and defensive capabilities that are integrated and concurrently planned. Effective IO planning requires a framework that focuses the staff, ensuring a plan that support's the commander's concept of operations by integrating the elements of IO into a coherent, synchronized plan. In a sense, defensive IO is the shield to protect our own systems and decision processes and offensive IO is the sword used against the adversary. But, our understanding of IO goes beyond attack and defend. It includes those actions taken to influence selected groups and decision-makers. It is necessary to include the integrative concept of perception management. Perception management combines truth projection, operations security, cover and deception, and psychological operations. It encompasses all actions taken to convey (or deny) selected information to an audience. The broad synchronization of; MAGTF PSYOP, Public Affairs, OPSEC, and deception fall within the concept of perception management. Perception management activities may have increased relevance during humanitarian assistance operations. It may be a key contributor to battlespace shaping efforts.

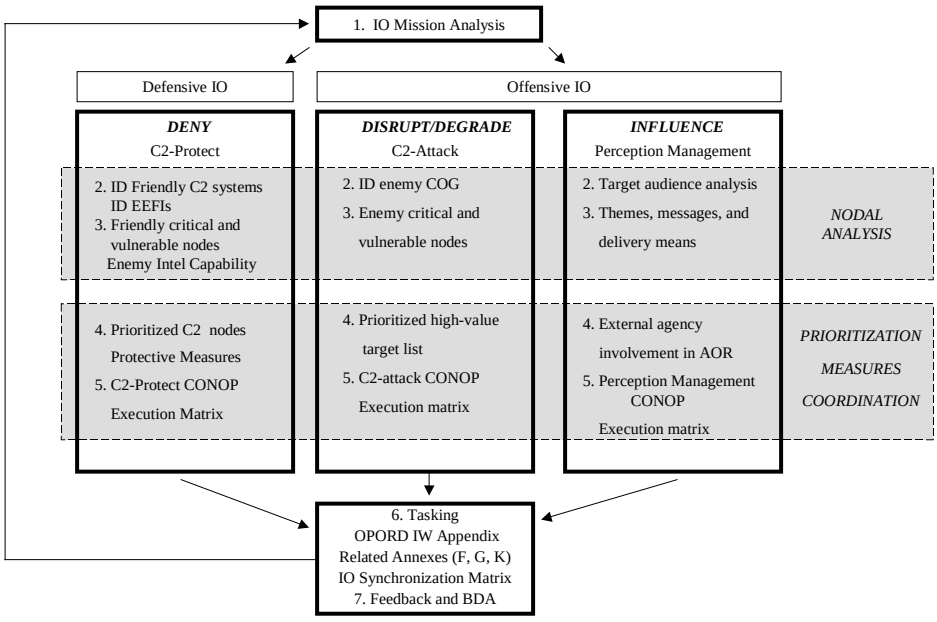

Figure 2-2. IO Planning Process.

An IO Planning Process provides a simple reference point for matching the logical analysis of C2 centers of gravity and key nodes to the MCPP. This helps keep IO planning "in step" with other planning efforts. It allows targets and tasks to be logically derived in a disciplined manner.

Target and intelligence analysis is essential in IO planning. Integration and planning efficiency is achieved by conducting IO

analyses simultaneously across functional areas. For example, nodal analysis is conducted simultaneously to determine key friendly nodes, key enemy nodes, and key target audiences. Then, each node (or center of gravity) is subsequently prioritized (according to commander's guidance), has specific IO measures (proposed tasks) placed against it, and is coordinated within the MAGTF operational scheme (reviewed by IO Cell and OPT). IO tasks and guidance form the basis for the IO/IW related OPORD sections. And, finally, the establishment of feedback mechanisms and BDA cycles permit the on-going evaluation of operations.

The underlying processes are twofold. First, all IO elements are logically analyzed to arrive at an executable COAs within the framework of staff planning. And, secondly, IO feedback mechanisms are put in place to create a repeatable loop of action, or sustainable IO process.

C2 Attack Planning Steps.

This seven-step process provides a structure that facilitates the planning process for C2-attack.

Step 1: Identify how offensive IO could support the overall mission and concept of operations. Identify available friendly assets and resource shortfalls. Develop IO CCIRs and PIRs.
Product: IO mission statement
MCPP Step: Mission Analysis

Step 2: Identify potential enemy C2 centers of gravity. Identify enemy electronic order of battle (EOB). Identify enemy C2 systems whose degradation will have a significant effect on enemy operations.
Product: Enemy potential C2 target list
MCPP Step: COA Development

Step 3: Analyze enemy C2 systems for critical and vulnerable nodes. Conduct risk assessment.
Product: C2 high value target list (HVTL).
MCPP Step: COA Development

Step 4: Prioritize the nodes for destruction.
Product: Prioritized high value target list.
MCPP Step: COA Development

Step 5: Determine desired effect and how the IO elements will contribute to the overall objective. Conduct intelligence gain/loss analysis.
Product: Offensive IO CONOP. IO-related no-strike list. C2-attack execution matrix.
MCPP Step: COA Development

Step 6: Assign assets to each targeted enemy C2 node.
Overall IO synchronization matrix. Subordinate unit tasks. IO Appendix.
MCPP Step: COA Development and Orders Development

Step 7. Determine the effectiveness of the operation.
Product: Battle Damage Assessment (BDA)
MCPP Step: Transition

C2-Protect Planning Steps.

This seven-step process provides a structure that facilitates the planning process for C2-protect.

Step 1: Identify how defensive information operations could support the overall mission and concept of operations. Identify available friendly assets and resource shortfalls. Develop IO CCIRs and PIRs.
Product: IO mission statement
MCPP Step: Mission Analysis

Step 2: By phase, identify critical friendly C2 systems that support the mission and concept of operations. Identify essential elements of friendly information (EEFI). Product: Friendly C2 list. EFFI list
MCPP Step: COA development.

Step 3: Determine enemy intelligence collection capability. Determine enemy capability to conduct C2-attack. Determine effects of friendly C2-attack on friendly C2 systems (mutual interference). Analyze friendly C2 systems for critical and vulnerable nodes.
Product: Identification of friendly critical and vulnerable nodes. Restricted frequency list (RFL).
MCPP Step: COA Development

Step 4. Prioritize friendly nodes for protection. Recommend protective measures for nodes.
Product: Prioritized list.
MCPP Step: COA Development.

Step 5: Finalize C2-protect CONOP.
Product: C2-protect CONOP. C2-protect execution matrix.
MCPP Step: COA Development.

Step 6: Assign subordinate unit tasks.
Product: C2-protect concept of operations. IW appendix. Overall IO synchronization matrix.
MCPP Step: COA Development and Orders Development.

Step 7: Monitor effectiveness of C2-protect plan.
Product: OPSEC, communication security assessments or information security assessments.
MCPP Step: Transition.

Perception Management.

Step 1: Identify how IO related activities (e.g. Public Affairs, Civil Affairs, PSYOP, Computer Network Operations) could support the overall mission and concept of operations.
Product: IO mission statement.
MCPP Step: Mission Analysis.

Step 2: Identify target audiences and analyze for vulnerability to external influence. Target audiences may include military and civilian leadership, populace, and media.
Product: Target audience analysis.
MCPP Step: COA Development.

Step 3: Identify themes, messages, delivery means.

Product: IO themes matrix.
MCPP Step: COA Development.

Step 4: Identify external agency involvement in AOR (e.g. NGO/PVOs).
Product: List of external agencies.
MCPP Step: COA Development.

Step 5: Identify IO synchronization requirements. Link IO/IW tasks to strategic and operational IO objectives. It may include external liaison requirements, operational phasing requirements, logistic support requirements, and go/no-go or ROE guidance.
Product: CONOP. Execution matrix.
MCPP Step: COA Development and Orders Development.

Step 6: Overall IO synchronization matrix. Assign subordinate unit tasks.
Product: Input to Public Annex F (Public Affairs) or Annex G (Civil Affairs). Input into Annex S (Special Technical Operations) or Annex B (Intelligence) Appendix 2 (Signals Intelligence). As required.
MCPP Step: Orders Development.

Step 7: Monitor IO activities within the AOR.
Product: IO Brief to MAGTF Commander.
MCPP Step: Transition.

Sustaining IO Operations.

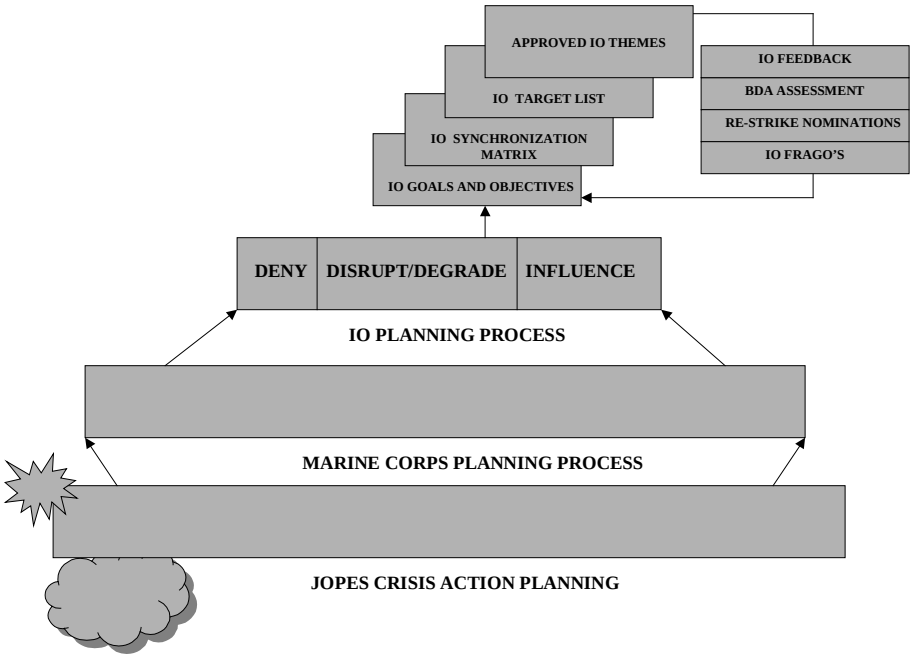

Figure 2-3. IO Planning and MCPP.

Having completed the MCPP steps and arrived at an executable course of action, the MAGTF IO Cell will be challenged to monitor the execution of the IO plan and recommend changes consistent with evolving

operations. The IO Planning Process is useful in providing IO support to the steps of the Marine Corps Planning Process (see figure 2-3). The IO Planning Process through offensive and defensive IO planning can help the MAGTF to develop the essential building blocks of:

- stated IO goals and objective;
- an IO synchronization matrix (which links mutually supporting IO actions);
- an IO target list;
- and, approved messages and themes to guide perception management activities.

These building blocks help sustain on-going IO operations. Sustained IO operations are supported by the MAGTF intelligence cycle, BDA cycle, targeting cycle, and the MAGTF operations battle rhythm. Taken together, these processes allow the MAGTF to gather and analyze feedback (intelligence cycle), assess the functional capability (or destruction) of enemy C2 nodes (BDA cycle), re-strike as necessary to maintain suppression of enemy C2 (targeting cycle), and modify and issue changes to on-going plans (operations battle rhythm). It is the IO Cell's participation in each of these cycles determines the daily IO battle rhythm. The logical transition from IO plan to IO battle rhythm is illustrated in figure 2-4. The IO process is now complete.

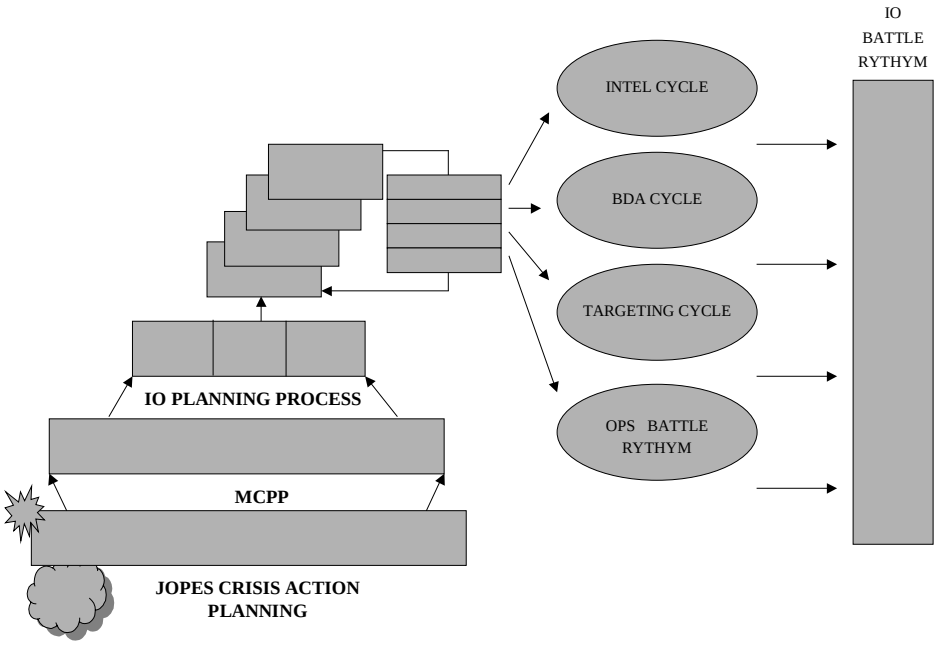

Figure 2-4. Transition from planning to battle rhythm.

CHAPTER 3
Elements of IO

Information Operations. Information Operations (IO) includes all actions taken to affect enemy information and information systems while defending friendly information and information systems. IO is conducted during all phases of an operation, across the range of military operations, and at every level of war.

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

Overview of Information Operation Elements. IO is composed of a variety of elements that must be employed together in an integrated strategy to be successful. Some of these elements appear more offensive or defensive, but it is their integration that ensures successful employment of IO in support of the MAGTF.

Deception

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

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

Definition. Military deception is action executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions, or inactions, that will contribute to the accomplishment of the friendly mission. The five categories of military deception are:

> Strategic military deception – Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support

the originator’s strategic military objectives, policies, and operations.

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

Tactical military deception – Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator’s objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.

Service military deception – Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems.

Military deception in support of operations security (OPSEC) – Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities.

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

Feint. A feint is a limited objective attack that involves contact with the enemy. A feint is an attack made at one place in order to distract the enemy’s attention away from the point of the main attack. Feints may: (1) vary in size from a raid to a supporting attack, (2) occur before, during, or after the main attack, and (3) may be independent of the main effort. Feints may be employed to cause the enemy to react in one of three predicable ways: employ his reserves improperly, shift his supporting fires, and reveal his defensive fires.

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

Ruse. A ruse is a trick of war to place false information in the enemy’s hand. Ruses are generally single, deliberate actions. It may be necessary to group several ruses together to ensure credibility of a deception story. Ruses are extremely susceptible to detection because of inconsistency and may present the enemy with a windfall of information that he is inclined to reject.

Display. A display is a simulation, disguise, or portrayal to project to the enemy the appearance of objects that do not exist

or appear to be something else. Displays include simulations, disguises, decoys, dummies. They may include the use of heat, smoke, electronic emissions, false tracks, and fake command posts.

Military deception in offensive IO. The adversary commander is the target for military deception in support of offensive IO. Some goals of military deception in offensive IO include:

- Achieve surprise.
- Preserve friendly forces, equipment, and installations from destruction.
- Minimize a physical advantage the enemy may have.
- Gain time.
- Cause the adversary commander 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.

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

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

The Deception Planning Process. See also Joint Pub 3-58, *Joint Doctrine for Military Deception.*

Step 1. Deception Mission Analysis. Conducted as part of overall mission analysis that is performed by the MAGTF following receipt of a new mission.

Step 2. Deception Planning Guidance. After mission analysis, the commander issues planning guidance to the staff. In addition to other planning guidance the commander states the deception objective for the operations.

Step 3. Staff Deception Estimate.

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

Step 4. Commander's Deception Estimate. The MAGTF Commander selects an operational deception COA for development into an operations plan and issues any additional guidance.

Step 5. Deception Plan Development. Developing the complete deception plan is the most time-consuming part of the deception planning process. There are five major actions in this step:

1. Complete the deception story.
2. Identify the deception means.
3. Develop the event schedule.
4. Identify feedback channels.
5. Develop the termination concept.

Step 6. Deception Plan review and approval. The commander reviews and approves the completed deception plan as part of the normal operation plan review and approval process. Need-to-know criteria remain in effect and only a limited number of personnel will participate in the deception plan review and approval process.

Special Considerations for Deception Planning.

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

Unintended effects. Third parties (e.g., neutral or friendly forces not read into the deception) may receive and act on deception information intended for the enemy. Deception planners should minimize the risk to other parties.

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

Deception and the Operations Order.

Tab A to Appendix 3 (IW) if Annex C (Operations) of the operations order is the Deception Tab. This tab implements the recommended course of action for Deception. It will detail the specific Deception tasks to be performed and will specify coordinating instructions for the control

and management of Deception missions. See Annex x for Deception Tab format.

Electronic Warfare

Definitions.

Electronic warfare (EW). Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or the attack the enemy. There are three divisions within EW: electronic warfare support (ES), electronic warfare attack (EA), and electronic warfare protection (EP).

Electronic Warfare Support (ES). The division of EW involving actions tasked by, or under direct control of an operational commander, to search for, intercept, identify and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. ES provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. ES data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT) and electronic intelligence (ELINT).

Electronic Attack. That division of EW involving the use of electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes jamming, deception, anti-radiation missiles, and the employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (i.e. lasers, RF weapons, particle beams).

Electronic Jamming. The deliberate radiation, re-radiation or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices, equipment or systems.

Electronic Deception. The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electronic dependent weapons, thereby degrading or neutralizing the enemy’s combat capability. Electronic deception includes: manipulative electronic deception, simulative electronic deception, and imitative electronic deception.

Directed Energy Weapons (DEW). A system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities and personnel.

Anti-Radiation Missiles (ARM). A missile which homes passively on a radiation source. These missiles use the electromagnetic emissions of a target for terminal guidance.

Electronic Protection (EP). That division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly of enemy employment of EW that degrade, neutralize, or destroy friendly combat capability.

Marine Corps EW Organizations. The Marine Corps has two types of EW units: the Radio Battalion and the Marine Tactical Electronic Warfare Squadron (VMAQ).

Radio Battalion. The mission of the Radio Battalion (RadBn) is to provide communications security (COMSEC) monitoring, tactical signals intelligence (SIGINT), EW, and special intelligence (SI) communications support to the MAGTF. There are two Radio Battalions. 1st RadBn is located at Kaneohe Bay, Hawaii and 2nd RadBn is located at Camp Lejeune, NC.

Marine Tactical Electronic Warfare Squadron (VMAQ). The VMAQs provide EW support to the MAGTF and other designated forces. The VMAQ conducts tactical jamming to prevent, delay, or disrupt the detection and tracking of enemy early warning, acquisition, fire or missile control, counter-battery, and battlefield surveillance radars. Tactical jamming also denies or degrades enemy communication capabilities. In addition, the VMAQ conducts electronic reconnaissance and ELINT operations. There are four VMAQs (designated VMAQ-1 through VMAQ-4) assigned to MAG-14, 2d MAW, Cherry Point, NC. Each squadron has five EA-6B Prowler aircraft.

Responsibility for Electronic Warfare. EW is the responsibility of the G/S-3. An electronic warfare officer (EWO) is normally appointed who is responsible for planning, coordinating, and tasking EW operations and activities. Other responsibilities include:

(1) Coordinate with the G/S-2 to establish priorities between electronic warfare and signals intelligence missions.

(2) Coordinate with the G/S-6 to facilitate maximum use of the electromagnetic spectrum through electronic protection and minimizing electromagnetic interference (EMI).

The EWCC. An Electronic Warfare Coordination Cell (EWCC) is a dedicated EW planning cell that may be established to coordinate EW activities.

Electronic Warfare Coordination Cell (EWCC). The MAGTF Commander will normally plan, synchronize, coordinate, and de-conflict EW operations through the electronic warfare coordination cell (EWCC). The EWCC facilitates coordination of electronic warfare operations with other fires and communications and information systems. This center coordinates efforts by the G/S-2, G/S-3, and G/S-6 to eliminate conflicts between these overlapping battlespace functions. The EWCC is under staff cognizance of the G/S-3. Assigned personnel identify potential conflicts in planned operations and work to resolve these issues. The EWCC includes an electronic warfare officer, a communications and information systems representative, and other liaison officers as needed. Liaison could include radio battalion representation, airborne

electronic countermeasures officers, a MACG radar officer, and other-Service representatives.

The term, Electronic Warfare Coordination Cell replaces Signals Intelligence/Electronic Warfare Coordination Center (S/EWCC) to coincide with the terminology used by other Services, and to better reflect the functions of the center. The EWCC is 'type' structure upon which to build Marine EW functions. It does not add structure to the existing organization, but rather is used to coordinate EW activities of personnel already assigned.

MAGTF staffs will provide personnel to incorporate an EWCC with the MEF G/S-3. Personnel will also be provided for liaison teams to higher headquarters EW coordination organizations when required, such as the Joint Commander's Electronic Warfare Staff (JCEWS) created by Joint Task Forces (JTFs).

EW and the Operations Order.

Tab B to Appendix 3 (IW) if Annex C (Operations) of the operations order is the EW Tab. It will detail the specific EW tasks to be performed and will specify coordinating instructions for the control and management of EW missions. See Annex x for EW Tab format.

Specific instructions for signals intelligence (SIGINT) is contained in Appendix 2 to Annex B (Intelligence). Defensive information warfare operations (IW-D) are contained in Tab G to Appendix 3 (IW) to Annex C (Operations). Information assurance (IA) activities are contained in Appendix 1 to Annex K (C4 Systems).

Operations Security

Operations Security. OPSEC is concerned with denying critical information about friendly forces to the enemy. Denial of critical information about friendly capabilities and limitations may result in flawed enemy command decisions. The intent of OPSEC is to force the enemy commander to make faulty decisions based upon insufficient information and to delay the decision process due to the lack of information. Although primarily associated with defensive IO, OPSEC contributes to offensive IO by slowing the enemy's decision cycle and providing opportunity for easier and quicker attainment of friendly objectives.

Definition. 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 adversary intelligence systems.
- Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

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

The OPSEC Process. OPSEC planning is accomplished through the OPSEC process. The OPSEC process has five distinctive steps that provide a framework for the systematic process necessary to identify, analyze, and protect information for essential secrecy. See Joint Pub 3-54, *Operations Security*.

(1) Identification of Critical Information.
(2) Analysis of Threats.
(3) Analysis of Vulnerabilities.
(4) Assessment of Risk.
(5) Application of appropriate OPSEC Measures.

OPSEC Responsibilities. The G/S-3 has primary responsibility for the OPSEC function. Normally, an OPSEC officer is appointed and is responsible to the G/S-3 for OPSEC planning and oversight. An OPSEC Working Group may be established to recommend OPSEC measures, coordinate or conduct OPSEC surveys, and write the OPSEC portion of the operations order.

OPSEC Support Agencies.

Counter-intelligence (CI) Teams. CI teams perform a wide range of duties such as security briefings, counter-sabotage, counter-espionage, and counter-surveillance inspections. CI measures enhance security; aid in reducing risks to a command; and are essential in achieving operational surprise during military operations. CI can provide a significant contribution to a unit's OPSEC program. CI personnel can support a command's OPSEC program by:

(1) Counter-intelligence Surveys
(2) Physical Security Evaluations
(3) Security Inspections
(4) Vacated Command Post Inspections
(5) Penetration Inspections
(6) Security Education

There is a CI team allocated to every MEF HQ. Also, see FMFM 3-25 *Counterintelligence*.

Force Imagery Interpretation Units (FIIUs). These units can provide a readout of overhead imagery and explain the signature your unit gives on the battlefield to adversary imagery systems. This type of product requires coordination through the G/S-2 and sufficient lead-time to obtain. A comprehensive OPSEC plan would ideally incorporate friendly imagery support to assist in the maintenance and improvement of OPSEC measures.

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

OPSEC and the Operations Order.

Tab C (OPSEC) to Appendix 3 (IW) of Annex C (Operations) of the operations order is the OPSEC Tab. This tab implements the recommended course of action for OPSEC. It will detail the specific OPSEC tasks to be performed and will specify coordinating instructions for the control and management of OPSEC missions. See Annex x for OPSEC Tab format.

Psychological Operations

Description. PSYOP are actions intended to convey selected information and indicators to foreign audiences. They are designed to influence emotions, motives, reasoning, and ultimately, the behavior of the enemy. At the operational level, PSYOP can include the distribution of leaflets, radio and television broadcasts, and other means of transmitting information that provides information intended to influence a selected group. It may be used to encourage enemy forces to defect, desert, flee, or surrender. At the tactical level, PSYOP include face-to-face contact, the use of loudspeakers and other means to deliver PSYOP messages. The mere presence of Marine forces maybe a PSYOP activity in itself, bringing influence on a situation through a display of purpose. PSYOP may support military deception operations.

Definition. Planned operations to, convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives.

Applications. PSYOP have strategic, operational, and tactical applications. See MCWP 3-36.2, *Psychological Operations*.

(1) At the strategic level, PSYOP may take the form of political or diplomatic positions, announcements, or communiques.

(2) At the operational level, PSYOP can include the distribution of leaflets, loudspeaker broadcasts, radio and television broadcasts, and other means of transmitting information that encourage enemy forces to defect, desert, flee, or surrender. Persistent attacks can amplify PSYOP effects, accelerating the degradation of morale and further encouraging desertion.

(3) At the tactical level, PSYOP include the use of loudspeakers and other means.

(4) PSYOP may also shape attitudes and influence behavior through face-to-face communication.

PSYOP Programs. A PSYOP program is an effort to produce a desired behavior in a target audience. A series of programs form a campaign to support the commander's goals. These goals may be political, economic, military, social, ideological, or religious. PSYOP programs include action programs, product programs, or product and action programs.

> Action Programs. Action programs are sequential, coordinated activities that may include military operations for their psychological impact. Examples range from military personnel repainting a local school, to an amphibious readiness group floating off a coast in a show of force.
>
> Product Programs. Product programs are sequential, coordinated presentations of visual, audio, and audiovisual products conducted for their psychological impact. Examples include leaflets, newspapers, news clips, and radio broadcasts. A product must attract the audience's attention and convey the intended meaning. The product must also lead the target audience in a direction that accomplishes our objective.
>
> Product and Action Programs. Product and action programs are a combination of the two types to produce a desired behavior in a target audience.

Perception management and PSYOP. PSYOP is only one of the means available to influence enemy attitudes and behaviors. All these related actions fall into a broad category called perception management. In various ways, perception management combines public affairs (the projection of the truth to the adversary and others), operations security (protecting friendly critical information), cover and deception (creation of misleading perceptions), and psychological operations.

Organization. The Marine Corps has no dedicated PSYOP units. However, support may be provided through the U.S. Army's 4th Psychological Operations Group (4th POG).

Employment. Since the approval authority for PSYOP is maintained by the supported CINC, ground commanders will receive operational and tactical PSYOP support (leaflets and broadcast operations) across their area of influence. The theater PSYOP plan includes this operational and tactical support and remains highly visible and thoroughly integrated into the MEF Commander's tactical plan. PSYOP staff officers at all levels will be made fully aware of the theater PSYOP campaign plan so that the MEF Commander retains a full understanding of the concepts concerning the theater PSYOP effort. However, development and coordination of campaigns and the production of PSYOP products does not occur at the MEF or MSC levels. The PSYOP assets assigned to these levels provide a tactical dissemination capability and have limited PSYOP product development assets. These limited assets are designed to respond to suggested products from the maneuver commander. Upon receiving a tactical commander's request for a product, the tactical PSYOP unit's developmental cells develop a product within the commander's intent. They then forward the suggested product, through

PSYOP technical channels to the senior PSYOP headquarters in the theater for further development and approval. Upon approval the product is produced and forwarded to the user level for dissemination.

MAGTF PYSOP actions must complement and support ongoing joint PSYOP activities. MEF personnel may come in contact with the target audiences far more frequently than the PSYOP specialists

PSYOP is an integrated non-lethal fire support asset. Planned PSYOP are generally conducted by special units attached to or in direct support (DS) of the MAGTF. The mere presence of U.S. Marines in a foreign country also has a significant psychological impact. Our behavior in turn may generate either negative or positive support from the local population. PSYOP will be planned by the MEF G-3 Future Operations and coordinated with public and civil affairs.

The enemy will most likely employ PSYOP to influence the local populace, attempt to weaken the will of U.S. forces (political and military), and attack the U.S. and world community popular support for the current contingency. MAGTF counteractions will be tailored to limit the enemy's opportunities to exploit the presence of U.S. Marines, and their actions, for PSYOP purposes. Detailed knowledge of the Host Nation's culture and individual self-discipline are required.

Responsibilities. Overall responsibility for the conduct of PSYOP falls under the cognizance of the G/S-3. A PSYOP Officer is provided for at the MEF G-3 Future Operations Section. If not provided for, a PSYOP officer may be appointed to provide control and management of the PSYOP effort and to meet liaison requirements.

The MAGTF will not normally identify, plan, or execute complex PSYOP (i.e. those requiring theme development, intricate target analysis, or the use of sophisticated media). These missions will be conducted by specially trained PSYOP units. However, the MAGTF Commander is responsible for providing PSYOP support and conducting tactical PSYOP (primarily through words and actions) in support of the MAGTF’s mission.

PSYOP Support Agencies.

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

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

The Air Force has the 193rd Special Operations Group of the Pennsylvania National Guard which flies the EC-130E Volant Solo. It provides an airborne radio and TV broadcast capability.

PSYOP and truth. To maintain credibility the U.S., by official policy, uses only the truth in its PSYOP. However, only selected information may be chosen for presentation in various ways, U.S. forces should never lie.

PSYOP and the Operations Order.

Tab D (PSYOP) of Appendix 3 (IW) to Annex C (Operations) of the operations order is the PSYOP Tab. This tab implements the recommended course of action for Deception. It will detail the specific PSYOP tasks to be performed and will specify coordinating instructions for the control and management of PSYOP missions. See Annex x for PSYOP Tab format.

Physical Destruction

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

Physical attack and destruction is the use of “hard kill” weapons against designated targets as an element of an integrated IO effort. Rules of engagement (ROE) will play a major role in determining if destruction is a viable option during a particular phase of the operation. Target planners may use physical destruction against both the command and control portions of the enemy’s C2 system. However, the enemy may be able to recover from physical destruction given sufficient time, resources, and redundancy. Planners must have some pre-planned measure of effectiveness with which to judge the results of physical destruction, and be prepared to monitor the target after the strike to determine status. C2 nodes identified as effectively reconstituted should be considered for re-attack if analysis determines that they are still critical in the overall IO effort. IO integration with the Battle Damage Assessment (BDA) cycle is essential. To preclude reconstruction, physical destruction should usually be timed for just before the enemy needs a certain C2 capability.

Physical Destruction and IO. Physical destruction falls within the application of traditional weapons targeting. See MCWP 3-16 (*Fire Support Coordination*). Physical destruction as an integrated part of IO should not be considered as only the systematic elimination of all enemy C2 systems. Total destruction of the hostile C2 system may not be attainable, desirable, or supportable. Friendly forces may need to use enemy C2 systems during the post-conflict phase of military operations. Careful selection and prioritization of C2 physical destruction targets builds the strongest case when competing against other type missions for weapons and delivery platforms.

Target Nomination. After the MAGTF Commander provides guidance as part of the planning process, targets are nominated to support the targeting objectives and priorities. IO planners should ensure that physical destruction targets are included with these target nominations. Through the nomination and review process, IO planners should ensure that IO-related physical destruction targets are included on the MAGTF Target List. Above all, IO targets must be presented as a cohesive,

integrated, and supporting target set that supports an operational requirement. For example, when planning SEAD, strikes against C2 systems should be coordinated with strikes against EW systems and command authorities. Or, if planning to isolate enemy forces, strikes against C2 systems and media should be coordinated with strikes against lines of communication.

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

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

No-strike list. Equally important to the target list is the no-strike list. Recommendations to this list should include nodes identified during intelligence gain/loss analysis. Also, the IO planner should identify those C2 or media elements within enemy territory that are hostile to the enemy regime and friendly to U.S. intentions. Friendly radio/TV broadcast facilities may be placed on a no-strike list. Finally, the IO planner should consider preserving infrastructure that will be of value once U.S. forces are ashore. A radio station or newspaper may be of use later by U.S. forces.

Timing. Physical destruction should be planned to support or coincide with friendly operational maneuver. Physical destruction should be timed for just before the adversary needs a certain C2 function to preclude reconstitution. After a strike the enemy may have only a short window of vulnerability before he is able to reform C2 systems or establish alternate communication paths.

Destruction Feedback. Battle Damage Assessment (BDA) analysis is essential to determine effectiveness of destruction efforts. For C2 targets, imagery that provides visual cues to destruction should be compared with other intelligence sources, such as signals intelligence, to determine target BDA assessment. C2 nodes must be functionally destroyed. A C2 node may be operational despite cosmetic structural damage. Another key concern is the enemy ability to reconstitute C2 nodes and re-establish effective command and control via alternate means. Re-strike may be required to maintain suppression of enemy C2.

Physical Destruction and the Operations Order.

Tab E (Physical Attack/Destruction) of Appendix 3 (IW) to Annex C (Operations) of the operations order is the Physical Attack/Destruction Tab. This tab implements the recommended course of action for destruction. It will detail the specific IO-related destruction tasks to be performed and will specify coordinating instructions for the

control and management of IO-related destruction missions if required. See Annex x for Physical Attack/Destruction Tab format.

Computer Network Operations

Definition.

Computer Network Operations (CNO) is an encompassing function that includes both the efforts to reduce effective enemy use of information networks and efforts to protect friendly information systems. Computer Network Attack (CNA) are operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. The MAGTF will not have an organic offensive CNA capability other than physical destruction, but it must be both aware of joint capabilities and be prepared to defend against the hostile CNA threat. Computer Network Defense (CND) is the use of defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. The planning of Computer Network Operations is another integrative function. CNA operations have an OPLAN Tab (Appendix 3, Tab C) of their own, while CND operations may be referenced in the IW Annex (Tab G, Defensive IO) and Information Assurance Appendix to the C4 Annex (Annex K).

Computer Network Attack is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. These objectives may be accomplished through physical destruction, electronic warfare, or some combination of these, and other capabilities, in an integrated IO effort. CNA targets may be attacked directly with these capabilities or by indirectly targeting supporting infrastructure. Depending on the circumstances or means involved, CNA may fall under the category of special information operations that require a special review and approval process.

CNA Planning Factors. Some CNA planning factors include:

(1) Requirements for specific resources to accomplish CNA.

(2) The need to identify security measures necessary to deny OPSEC indicators to enemy intelligence and /or computer network defense (CND) efforts.

(3) Establishing prior coordination and precautions necessary to govern use of CNA to ensure continued effective operations in support of the commander’s objectives. This includes establishing rigorous targeting, legal, and intelligence gain/loss review procedures with appropriate sections of the Joint staff, theater CINC, supporting organizations, and higher authority.

(4) CNA requires specific and detailed intelligence in order to be successfully executed. CNA planners must work with intelligence planners to ensure that Annex B (Intelligence) contains sufficient guidance to allow intelligence personnel to adequately support CNA. Coordination with intelligence planners should include a frank appraisal of what intelligence can reasonably be expected, given the time and resources available.

(5) Amount of lead-time available. CNA efforts normally require substantial lead-time. This requirement is driven by (a) the need for detailed intelligence support; and (b) the need to sometimes prepare and integrate CNA techniques based on the intelligence support.

(6) Identification of supported and supporting commands and agencies. Many technical aspects of CNA may be executed by supporting commands and agencies. CNA may have unique interagency review requirements. Clarification of roles and responsibilities of all concerned is a crucial aspect of CNA success.

(7) CNA planning will require coordination with appropriate government agencies for reconnaissance and targeting approval through the chain of command.

Responsibilities. Within the MEF, CNA planning is normally accomplished through the IO cell imbedded within G-3 Future Operations. It is coordinated with other offensive IO activities such as EW, PSYOP, military deception, OPSEC, and physical destruction.

Computer Network Attack (CNA) and the Operations Order.

Tab F (Computer Network Attack) of Appendix 3 (IW) to Annex C (Operations) of the operations order is the CNA Tab. This tab implements the recommended course of action for destruction. It will detail the specific IW related CNA tasks to be performed and will specify coordinating instructions for the control and management of IW-related CNA missions if required. See Annex x for CNA Tab format.

CNA plans should:

(1) Identify the desired effect(s) that CNA is to accomplish. The effect(s) desired may be to disrupt, deny, degrade, or destroy information or information systems at one or more physical locations. These effects may achieve the operational objectives or they may support one or more of the other IO elements. The desired effect drives such planning elements as timing, sequencing, means, and priority of effort.

(2) Identify risks associated with CNA. Risks to be discussed include: collateral damage (to other networks or to other information within the same network), discovery and /or attribution (in the case of sensitive information operations), fratricide (to US or allied/coalition networks or information), and possible conflict (with CND, Computer Network Exploitation (CNE), and other CNA activities). Policy and rules of engagement (ROE) guidance is applicable.

(3) Evaluate the enemy’s ability to detect, counter, and respond to CNA. Identify back-up or contingency actions that are to be taken in the event of detection or counter-actions. Coordinate such actions with other IO capabilities planners and ensure such actions are addressed in other sections of the OPLAN. Coordinate with G/S-2, G/S-3, G/S-6 on information assurance measures and preparations in anticipation of a possible counter-attack.

(4) Identify differences in procedural, review, and approval processes between a CNA effort initiated as part of the offensive IO effort and CNA actions taken in response to a detected enemy CNA. Failsafe procedures must be established when responding to enemy CNA to ensure that the true origin of the attack had been identified, since this is essential in determining DOD authority to respond to an attack.

(5) Identify measures of effectiveness. The executing organization is probably in the best position to measure the effectiveness of an attack. The plan must identify means to verify the target, impact, and damage immediately. The Intelligence Community may be able to support the damage assessment with indirect means. How CNA success is measured may also affect how supporting commands and agencies plan and execute CNA. Measures of effectiveness must be stated in a way that can be supported by the given CNA, intelligence, and other supporting resources. For example, measuring effectiveness as a "percentage of enemy computers (or C2, etc) destroyed" may not be realistic if either the total number (100%) cannot be determined or if timely BDA of ongoing degradation of capability cannot be obtained.

(6) Identify special resources required to conduct the CNA effort.

(7) Integrate CNA with other military actions, the destruction plan, and other IO elements to achieve synergistic effects.

Defensive Information Operations

Definition. The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Defensive Information Operations is a broad functional area that includes Information Assurance, Computer Security, and Information Security activities.

The Defensive IO Implementation Process. Warfighters depend upon information to plan operations, deploy forces, and execute missions. However, increasing dependence on new technologies makes forces more vulnerable. Defensive information operations ensure the necessary protection and defense of information and information systems that MAGTFs depend upon to conduct operations. Four interrelated processes comprise defensive IO (IO-D):

(1) Information environment protection;
(2) Attack detection;
(3) Capability restoration;
(4) Attack Response.

Defensive IO integrates and coordinates protection and defense of information, information-based process (including human decision-making processes), and information systems (including command, control, communications, and computer (C4I) systems, weapons systems, and

critical information infrastructure systems, etc). The defensive IO process is an integral part of deterrence and force protection.

IO-D and IO. Many areas within IO can contribute directly and indirectly to defensive information operations.

Information Assurance. Information Assurance (IA) capabilities help ensure the availability, integrity, identification and authentication, and confidentiality, and non-repudiation of friendly information and information systems while denying adversary access to the same. IA capabilities include:

INFOSEC. Information System Security (INFOSEC) is the protection of information systems against unauthorized access or modification of information, whether in storage, processing or transit, and against denial of service to authorized users. INFOSEC includes measures necessary to detect, document, and counter such threats. INFOSEC is composed of the following two disciplines:

COMPUSEC. Computer security (COMPUSEC) involves the measures and controls that ensure confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

COMSEC. Communications security (COMSEC) includes measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, transmission security (TRANSEC), emission security, and physical security of COMSEC material.

Security. Personnel security and physical security are examples of procedures contributing directly to information protection.

Operations Security (OPSEC). OPSEC is a process that identifies critical information and subsequently analyzes friendly actions attendant to military operations and other activities, and then implements procedures to prohibit disclosure of critical information to the enemy.

Counterintelligence (CI). CI activities integrate and coordinate protection and defense of information and information systems. CI support to defensive IO includes collection focused on indications and warnings and the identification of threats to information and information systems; investigations of computer-based crimes; and analysis of production support to policy, plans, operations, acquisition, and force protection.

Electronic Warfare (EW). Defensive EW procedures known as electronic protection (EP), including communications security (COMSEC) procedures, changing callsigns/words and frequencies, antenna and communications site positioning, are examples of procedures and disciplines directly contributing to information and information system protection. Others include COMPUSEC, OPSEC, and personnel information access controls.

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

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. Procedures and actions to minimize loss or degradation of information, once discovered, are also an important part of risk management.

Intelligence. Intelligence provides an understanding of the threat to information and information systems by identifying potential information adversaries, their intent, and their known and assessed capabilities.

Public Affairs and Command Information. These programs contribute to information protection by disseminating factual information. Factual information dissemination counters adversary deception and psychological operations.

Vulnerability Analysis and Assistance. A program conducted by friendly forces to identify vulnerabilities in information systems and to provide an assessment of their effects on information access and availability. The Defense Information Systems Agency (DISA) operates a program known as the Vulnerability Analysis and Assistance Program (VAAP) specifically focusing on automated information systems vulnerability. The National Security Agency (NSA) has a COMSEC monitoring program that focuses on telecommunication systems using wire and electronic communications.

Responsibilities. Overall responsibility for the conduct of Defensive Information Operations falls under the cognizance of the G/S-6. However, coordination with the G/S-3, MAGTF EWO, and IO Cell (if established) is required.

Support Agencies.

Headquarters Marine Corps.

Information Assurance (IA) Branch (HQMC/C4/CP/IA).

Information Assurance (IA) Training & Certification. HQMC/C4/CP/IA oversees the Marine Corps IA certification program. This program is based on the Computer Security Act of 1987 (Public Law 100-235) which requires *"Each Federal agency shall provide for the mandatory periodic*

training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation 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 downloaded from the HQMC/C4/CP/IA web site. The downloaded certificate must be signed by the System Administrator's Commanding Officer and G-6, (W)ISMO, or ISSO. Upon signing, the certificate can be delivered by the System Administrator to Marine Corps Manpower to be permanently recorded into the System Administrator's personnel record. Viewed from a macro-level, Manpower will use the certificate to better understand the Marine Corps' security preparedness. Viewed from a micro personal level, Manpower will use the certificate for review by selection boards and for tracking a System Administrator's technical proficiency and professional growth.

The Marine Corps Information Technology and Network Operations Center (MITNOC). Located in Quantico, VA, the MITNOC provides continuous, secure, global communications; and operational sustainment and defense of the Marine Corps Enterprise Network (MCEN) for Marine Forces World-wide to facilitate the exchange of information across the Defense Information Infrastructure (DII).

The MITNOC exists to supply customer support to the Marine Corps Enterprise Network and maintains a 24 hour, 365 day a year helpdesk Marine customers to place trouble tickets.

If a System Is Compromised: Reporting a virus hit OR a threatening attempt to access your system is crucial. When the hit or attempt occurs contact your local Information/Computer System Security Officer (ISSO/CSSO) to obtain immediate assistance. Be sure that you initiate your initial report according to your local/regional base or station's guidance. At minimum, contact the MITNOC Helpdesk to report the incident.

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

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

The Marine component to the JTF-CND is the Marine Forces Computer Network Defense (MARFOR-CND), which is collocated with the MITNOC at Quantico, VA. The MARFOR-CND is responsible for the defense of the Marine Corps Enterprise Network (MCEN) and other USMC computer networks connected to the Defense Information Infrastructure (DII) from strategic Computer Network Attacks (CNA) and other CND missions as directed by the JTF-CND. The MARFOR-CND is responsible for the collection of data on CNA against the MCEN and other USMC computer networks, formulating courses of action (COA) to thwart CNAs, coordinating and directing USMC actions for defense, and prioritizing recovery actions.

Computer Emergency Response Team (CERT). The Service CERT for the Marine Corps is Marine Corps Intrusion Detection and Analysis Section (MIDAS), which is an element of the MITNOC located in Quantico, VA. The MIDAS section provides real-time, 24 hour, observation of the MCEN for network and host based intrusion incidents based upon a specified criteria. Valid incidents are analyzed from strategic and operational perspectives for impact upon the MCEN. This data is also warehoused to provide MARFOR-CND with usable information to perform incident profiling, trend analysis, and predictive analysis. The MIDAS section provides guidance and support to Marine Corps organizations vulnerability testing, and malicious code incident response teams.

Regional Computer Emergency Response Teams (RCERT). DISA RCERTs are functionally and organizationally embedded within five DISA Regional Network Operations and Security Centers (RNOSCs) to provide a comprehensive picture of status of network assets, along with near-real-time data on network anomalies and intrusive behavior. RCERTs provide CND support to CINCs, Services, Agencies and Local Control Centers. RCERTs are responsible for intrusion detection, monitoring, vulnerability analysis, and computer security incident handling and reporting within its Area of Responsibility (AOR). Each RCERT is the responsible agent for the resolution of computer security events and incidents within its AOR. The RCERTs are staffed with computer security engineers and provide telephonic, on-line, and on-site support fulltime to resolve computer security problems.

DISA VAAP. The Defense Information Systems Agency (DISA) operates a program known as the Vulnerability Analysis and Assistance Program (VAAP) specifically focusing on automated information systems vulnerability. Upon customer request, the VAAP collects, identifies, analyzes, assesses and resolves INFOSEC vulnerabilities.

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

INFOSEC Program Management Office (IPMO). The IPMO is a joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) organization charged with the execution of the Defense Information Security Program. The primary responsibility of the joint program office is to assure the effective and coherent application to the overall Defense Information System, and its individual component parts, e.g., the Defense Information System Network (DISN), the Defense Integrated Secure Network (DISNET), the Defense Data Network (DDN), the

Defense Message System (DMS), the Interoperable Tactical/Strategic Data Network (ITSDN), and the Defense Data Centers.

Defensive Information Operations (IO-D) and the Operations Order.

Tab G (Defensive Information Operations) of Appendix 3 (IO) to Annex C (Operations) of the operations order is the IO-D Tab. This tab implements the recommended course of action for IO-D. It will detail the specific IO-related IO-D tasks to be performed and will specify coordinating instructions for the control and management of IO-related IO-D missions. See Annex x for IO-D Tab format.

Related Information Operation Activities.

Related activities are operations that are neither offensive nor defensive in nature but must be coordinated with all other IO/IW efforts. Such activities include public affairs (PA) and civil military operations (CMO). PA and CMO are pervasive and continuous. MAGTFs may find PA and CMO on-going within their operational area as part of an international, national or CINC engagement or battlespace shaping initiative. Activities already on-going in the battlespace will affect MAGTF IO initiatives.

Public Affairs.

PA consists of those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense (DOD). These activities expedite the flow of accurate and timely information to internal and external audiences. As a supporting IO element, PA allows the MAGTF to inform the enemy about the command's intent and capabilities. As a matter of U.S. policy, PA activities will not be used to provide disinformation to either internal or external audiences. See MCWP 3-33.1, *Marine Corps Public Affairs*.

Civil Military Operations.

Civil Military Operations, executed by Civil Affairs units, are the activities of a command that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. CMO may include performance by military forces of activities and functions normally the responsibility of local government. CMO and PSYOP are mutually supportive within civil-military operations. CMO can assist to support friendly or host nation (HN) civilian welfare, security, and developmental programs, while PSYOP can publicize the existence or success of these activities to generate target population confidence in and positive perception of U.S. and HN actions. See MCWP 3-33.1, *MAGTF Civil-Military Operations*.

ANNEX X
INFORMATION OPERATIONS CELL

1. Purpose. This annex provides a description of the IO Cell and the responsibilities of its members.

2. Description.

The IO cell is a task-organized group of individuals brought together within a MAGTF and higher headquarters to focus a variety of separate disciplines and functions on IO for the command. A fully functioning IO cell integrates a broad range of potential IO actions and related activities that contribute to accomplishing the mission. Ensuring that IO is an integral part of all operations requires extensive planning and coordination among all the elements of the staff. The IO cell is the mechanism for achieving that coordination.

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

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

3. Responsibilities.

a. IO Cell, as a whole.

(1) Plan the overall IO effort including preparation of the IW appendix (Appendix 3 to Annex C, Information Warfare) to the MAGTF OPORD. Coordinate to ensure synchronization with Annex K (C4), Annex F (Public Affairs) and Annex G (Civil Affairs).

(2) Develops offensive and defensive IO concepts.

(3) Recommends IO priorities.

(4) Coordinates subordinate IO plans.

(5) Coordinates the planning and execution of IO activities between organizations responsible for each IO element.

(6) Coordinates nodal analysis and compiles IO target list. Submits IO targets for inclusion in MAGTF targeting plans.

(7) Ensures OPSEC plan provides necessary C3 protection and is coordinated with deception plan and operations.

(8) Ensures other IO elements support the deception effort.

(9) Ensures PSYOP themes support, and are supported by, the other IO elements.

(10) Coordinates intelligence support to all IO elements.

(11) Coordinates and de-conflicts IO operations with Special Information Operations (SIO) and Special Technical Operations (STO).

(12) Recommends additions, deletions, and modifications to ROE.

b. IO Officer.

(1) Responsible to G-3 for all MAGTF IO.

(2) Ensures IO input provided to OPT during planning.

(3) Oversees core personnel within the IO cell and calls plenary IO cell meetings that include external support augmentees as appropriate.

(4) Coordinates all IO matters with higher, adjacent, and subordinate units.

(5) Requests external support from, and coordinates IO activities with, external agencies (i.e. JIOC, JWAC, NSA, DIA, JCMA, SPACECOM, etc).

c. Intelligence (G-2) member.

(1) Provides timely and directed intelligence support to IO.

(2) Advises on EOB, enemy TP, enemy commander profiles, etc.

(3) Reconciles restricted targets on RFL.

(4) Provides BDA and effectiveness feedback for IO activities.

d. C4 (G-6) member.

(1) Provides information on SIGSEC and COMSEC efforts and recommends adjustments.

(2) Identifies critical C4 nodes for defensive IO protection.

(3) Provides protected and restricted frequencies to the RFL.

(4) Coordinates and reports on JCMA monitoring of MAGTF C4 architecture.

e. OPSEC Officer.

(1) Oversees overall OPSEC efforts.

(2) Develops and updates the OPSEC plan.

(3) Initiates an OPSEC feedback program to monitor OPSEC effectiveness.

(4) Coordinates all OPSEC activities with external agencies.

f. PYSOP Officer.

(1) Maintains a thorough knowledge of all PSYOP plans and actions.

(2) Provides expert advice on PSYOP matters.

(3) Coordinates PSYOP plans, actions, and support with other IO elements, especially OPSEC and deception.

g. Deception Officer.

(1) Heads Deception Cell, if established.

(2) Coordinates development and update of deception plan, to include obtaining higher level authority if required.

(3) Monitors and controls dissemination of deception related information. Ensures security of material is maintained.

(4) Coordinates Deception plans with other IO elements.

(5) Coordinates with G-2 for feedback on deception success.

(6) Monitors and controls execution of the deception event schedule.

h. EW Officer.

(1) Oversees the EW Coordination Cell (EWCC) under the direction of the G-3.

(2) Prepares EW plans.

(3) Coordinates EW operations with internal units and external agencies.

(4) Coordinates EW operations with the other Io elements.

(5) Establishes and maintains the RFL in concert with the G-6.

i. SIO/STO Officer.

(1) Plans, coordinates, and de-conflicts SIO/STO activities.

(2) Allows at least two officers within the IO cell (IO Officer and SIO/STO Officer) to have situational awareness over SIO/STO activities.

(3) Conducts liaison with higher SIO/STO representatives to facilitate coordination and release and execution authority for SIO/STO.

j. Counter-Intelligence (CI) Officer.

(1) Assesses defensive IO posture from a CI perspective.

(2) Recommends corrective actions.

k. Targeting representative.

(1) Provides entry for IO targets into the targeting cycle.

(2) Ensures IO targets are given proper consideration in the targeting process.

(3) Provides IO Cell recommendations to the restricted target list.

l. Other representatives.

(1) Attend IO Cell sessions as invited by IO Officer.

(2) Provide expert advice and opinions.

(3) Coordinate with parent organizations in support of MAGTF IO.

ANNEX X
MAGTF INFORMATION WARFARE ASSETS

CI/HUMINT Company.

The CI/HUMINT company conducts HUMINT, CI, and interrogator-translator operations in support of IO. This support encompasses the full range of tactical CI and HUMINT operations, including screening operations, interrogation/debriefing of prisoners of war and persons of IO interest, conduct of CI force protection source operations, conduct of CI surveys and investigations, preparation of CI estimates and plans, translation of documents, and limited exploitation of captured material. In addition to the specialized CI and interrogator-translator platoons, the company employs task-organized HUMINT exploitation teams in direct support of MAGTF subordinate elements. HUMINT exploitation teams combine CI specialists and interrogator-translators in one element, thereby providing a unique range of CI/HUMINT services to the supported unit. Additionally, a Naval Criminal Investigative Service agent is normally assigned to the CI/HUMINT company.

Radio Battalion.

The radio battalion provides ground-based SIGINT, EW, communications security monitoring, and special intelligence communications capability to support MAGTF operations. In addition to directing the employment of its subordinate elements, the radio battalion is the focal point for MAGTF ground-based SIGINT operations, providing SIGINT, EW, special intelligence communications, COMSEC monitoring, and component headquarters deployable communications. NSA-funded projects have led to fielding and improvements to the Team Portable Communications Intelligence System, the technical control and analysis center, and the Mobile Electronic Warfare Support System. Other initiatives include improvements to the radio battalions' radio direction-finding capability, special intelligence communications, and signal intercept capability under the Marine Corps/NSA Radio Battalion Modernization and Concept Exploration Project.

Civil Affairs.

The Marine Corps CA organizations are limited to two CAGs that augment the capability of the MAGTF. The CAGs, when activated, are capable only of self-administration and require support from the MAGTF command element's support unit in such areas as supply, health services, mess, and transportation. A CAG is capable of minimum essential civil-military functions necessary to support the assigned missions of the MAGTF and are usually, entirely civil-military operational in nature. CA activities will normally include civic action, public health, disaster relief, and humanitarian-assistance programs. They can be tailored to stability operations to promote HN self-sustaining capabilities and to limited objective operations against specific targets. The force service support groups can also provide CA trained personnel to MAGTF command elements to assist in the planning and conduct of CA activities.

Psychological Operations.

The Marine Corps has no dedicated PSYOP units. However, a MAGTF has a limited capability to execute observable actions to convey selected impressions to support PSYOP objectives.

Marine Tactical Electronic Warfare Squadron.

The mission of the VMAQ squadrons is to conduct airborne EW in support of MAGTF and joint operations. VMAQs are structured into four active force squadrons (VMAQ-1, 2, 3, 4) with at least five aircraft each. This structure provides the flexibility necessary for continuing to support peacetime requirements, as well as the capacity to concurrently assign Marine EA-6B forces to commanders in different areas of operation.

The Tactical Electronic Reconnaissance Processing and Evaluation System (TERPES) AN/TSQ-90D (V) system is required by EA-6B aircraft to provide EW analysis and reporting. TERPES has the capability to process digital electronic warfare support measure (ESM) data collected and electronic countermeasures data recorded by the EA-6B aircraft. It develops, maintains and distributes a tactical electronic order of battle via data link or secure voice interfaces with AN/MSC-63A Tactical Communications Central, Tactical Aircraft Mission Planning System, Tactical Data Information Exchange Service, and the TADIL A (Link 11) or TADIL B (Link 11B) networks. The processed ESM data results in electronic intelligence that is used to determine the extent of the enemy threat and to provide electronic reconnaissance reports to tactical commanders for further planning.

Annex X: External IO Organizations

Organization	Location	Description
USSPACECOM	Peterson AFB, Colorado	DoD lead for Computer Network Defense (CND) and Computer Network Attack (CNA) activities.
Joint Information Operations Center (JIOC)	Kelly AFB, TX	Provides comprehensive Information Operations support to the Joint Force Commander and facilitates the integration of IO into military operations. Supports planing, coordination, and execution of DoD IO worldwide.
4th Psychological Operations Group (POG)	Fort Bragg, NC	The 4th POG (Airborne) is the only active Army PSYOPs unit.
National Air Intelligence Center (NAIC)	Wright-Patterson AFB, Ohio	Primary DoD producer of foreign aerospace intelligence. Assesses foreign capabilities, develops targeting and mission planning intelligence materials, and evaluates evolving technologies of potential adversaries.
Joint Warfare Analysis Center (JWAC)	Dahlgren, VA	Primarily responsible for the integration and analysis of scientific and technical data related to warfare planning against infrastructure networks of selected countries of interest. Supports military operations and recommendations for deliberate and crisis planning. Products include high-leverage targeting options directed at enemy infrastructure (electric power, petroleum, oils and lubricants, lines of communications and telecommunications). Also tasked with evaluating weapon's capabilities against critical components of selected targets; assess the effects attacks on infrastructure networks have on the abilities of an enemy's

		fielded forces to conduct offensive or defensive operations; provide input from this analysis to intelligence organizations and provide battle damage assessment indications for network and critical node failure analysis through the JCS.
Information Operations Technology Center (IOTC)	Fort Meade, MD	A joint DoD/Intelligence Community Center of Excellence tasked with developing and maintaining a computer/network technology-based tool box of techniques and applications for the warfighter.
Joint COMSEC Monitoring Agency (JCMA)	Fort Meade, MD	The JCMA is a field operating agency of the Joint Chiefs of Staff. It was created in 1993 by a Memorandum of Agreement between the Service Operations Deputies and Directors of the Joint Staff and NSA. The JCMA is charged with conducting "COMSEC monitoring (collection, analysis, and reporting) of DOD telecommunications and automated information systems (AIS) and monitoring of related noncommunications signals
Fleet Information Warfare Center (FIWC)	Little Creek Amphibious Base, Norfolk, VA	Established as the Fleet CINC's authority for developing IW/C2W related tactics, procedures and training, and for identifying requirements for IW/C2W RDT&E, acquisition, training and fleet staff augmentation. Also maintains a Navy Computer Incident Response Team.
Information Warfare Support Cell (IWSC/P42)	Fort Meade, MD	Provides information support, targeting, analysis, assessments, and intelligence gain/loss assessments. Also serves as the Special Technology office for NSA.

		Provide IW operational support to land component and separate Army commands; and to facilitate planning and execution of Information Operations.
Land Information Warfare Activity (LIWA).	Fort Belvoir, VA	Coordinates, arranges and synchronizes IW intelligence and counterintelligence support to land component commands, and deploys field support teams to assist and support land component commanders in C2 matters.
Defense Information Systems Agency (DISA)	Washington, DC	DoD agency responsible for information technology and central management of major portions of the Defense Information Infrastrucute (DII). Mission: to plan, engineer, develop, test, manage programs, acquire, implement, operate and maintain Information Systems for C4I and mission support under all conditions of peace and war. Has defensive IO responsibilities.
Information Systems Security Office (ISSO).	Fort Meade, MD	Provides Information Protection products and services for DoD and other government information systems. Provides technical vulnerabilities and threat assessments when tasked.
National Security Agency (NSA)	Fort Meade, MD	The National Security Agency (NSA)/Centraol Security Service (CSS) is responsible for the centralized coordination, direction, and performance of highly specialized technical functions in support of U.S. Government activities to protect U.S. communications and produce foreign intelligence information.

Naval Information Warfare Activity (NIWA).	Washington, DC	The Navy's principal technical agent and interface to service and national level agencies engaged in IW technologies. Also acts as primary technical interface with FIWC (Fleet Information Warfare Center) for the transition of IW special technical capabilities for naval and Navy-supported joint operations. Conducts technical threat analysis and vulnerabilities assessment to develop requirements for evaluating new information technologies, competitive architectures, and advanced concepts for offensive and defensive IW systems.
Joint Spectrum Center (JSC)	Severn River Naval Complex, Annapolis, MD	A DISA Field Activity and DoD center of excellence for electromagnetic spectrum management matters supporting the Joint Staff (J-6). Assists in managing Joint Restricted frequency List and resolving interference and jamming incidents.
Joint Communications Support Element (JCSE)	MacDill AFB, Florida	A deployable tactical communications unit under the operational control of the Joint Staff. Provides Chairman, Joint Chiefs of Staff (CJCS)-directed contingency and crisis communications to meet operational and support needs of the Joint Chiefs of Staff (JCS), Services, Unified Commands, Defense Agencies, and non-Defense agencies.

ANNEX X
IO PLANNING CHECKLIST

PLAN AND INTEGRATE INFORMATION OPERATIONS

Purpose: IO plans integrate aspects of Operations Security (OPSEC), military deception, Psychological Operations (PSYOP), Electronic Warfare (EW), destruction, Computer Network Operations (CNO), and Defensive IO to deny enemy information it needs to make operational decisions, influence operational decisions the enemy makes, and degrade or destroy an enemy's Command, Control, Communications, Computers, and Intelligence (C4I) systems. IO plans also protect friendly Command and Control (C2) systems and processes. Planning and integration is normally conducted by an IO cell, consisting of representatives from planning cells for each of the IO elements; OPSEC, military deception, EW, PSYOP, destruction (targeting), CNO, Defensive IO. In addition, representatives from the G-6, Public Affairs Office, Civil Affairs, or from special planning cells may be present.

STEPS

1. Conduct IO mission analysis.

   a. Determine known facts related to IO.
      (1) Define area of interest.
      (2) Review intelligence estimates.
      (3) Identify intelligence shortfalls.
   b. Determine enemy IO centers of gravity.
   c. Develop assumptions related to IO.
   d. Analyze higher mission and MAGTF mission for IO implications.
   e. Determine IO operations limitations.
      (1) Things IO must do.
      (2) Things IO cannot do.
   f. Identify/determine IO tasks. Specified, implied, essential.
   g. Analyze requirement for IO in MAGTF operations.
      (1) Establish offensive IO goals.
      (2) Establish defensive IO goals.
   h. Conduct resource analysis to determine of sufficient assets are available to accomplish tasks.
   i. Conduct initial IO risk assessment.
   j. Determine IO endstate.
   k. Draft the IO mission statement.

2. Receive MAGTF Commanders planning guidance.

3. Develop initial IO staff estimate. The purpose of the staff estimate is to determine whether the mission can be accomplished and which COA can best be supported.

   a. Incorporate Mission Analysis results.
   b. Identify IO Subject Matter Experts (SME).
   c. Identify resource shortfalls.
   d. Identify external support requirements.

4. Develop IO options to support MAGTF COA development.

   a. ICW G-2, conduct nodal analysis for offensive IO.
      (1) Identify enemy C2 systems.
      (2) Identify enemy centers of gravity.
      (3) Conduct nodal analysis of enemy systems.
          (a) Identify critical nodes.
          (b) Identify vulnerable nodes.

   b. Conduct analysis of friendly C2 for defensive IO.

(1) Awareness of vulnerabilities and identification of appropriate defensive measures.
(2) Analyze enemy offensive IO capability:
(a) Enemy intelligence systems.
(b) Enemy HQ/staff facilities.
(c) Enemy component units, equipment, facilities that would employ IW against friendly C2.
(3) ICW G-6, conduct nodal analysis for friendly systems.
(a) Identify critical nodes.
(b) Identify vulnerable nodes.
(4) Identify friendly centers of gravity.

c. Develop a consolidated list of critical and vulnerable nodes.
(1) Enemy nodes for offensive IO planning.
(2) Friendly nodes for defensive IO planning.

d. Prioritize the consolidated list of critical and vulnerable nodes.
(1) Reflect enemy/friendly centers of gravity.
(2) Determine desired effect on each node. Deny, disrupt, degrade, influence.

e. Develop IO COAs.
(1) Identify options for accomplishment of offensive IO goals.
(2) Identify options for accomplishment of defensive IO goals.
(3) ICW G-3/Operational Planning Team (OPT), integrate IO COAs.
(4) Begin development of IO synchronization matrix.

5. Participate in COA analysis. Participate in COA analysis. Be prepared to contribute to the process of wargaming by mentally 'fighting the battle' in time and space. The process may use the structure of action-reaction-counteraction sequences for critical events. Analyze IO concepts, wargame within the context of other IO COAs and the overall MAGTF scheme of maneuver. Determine:
a. If more specific forces are required.
b. If more specific assets/resources are required.
c. Branches and sequels to IO operations.
d. Unintended effects.
e. Assess IO risks.
f. Provide input to Time-Phased Force and Deployment Data (TPFDD) development.

6. Participate in IO COA comparison.

a. Participate in determining the criteria for comparing COAs. Criteria for IO operations should come from:
(1) Commander's intent/guidance.
(2) Factors of METT-T (mission, enemy, terrain, troops, time).
b. Ensure recommendations for IO have been coordinated with operational maneuver.

7. Develop/coordinate the IO plan.

a. Plan OPSEC in support of IO.

(1) Plan OPSEC for offensive IO.
(a) Plan OPSEC against enemy operational level commander(s).
(b) Plan OPSEC against enemy control systems.

(2) Plan OPSEC for defensive IO.

(a) Plan offensive OPSEC. Attack enemy intelligence collection systems using destruction or Electronic Attack (EA) means.

(b) Plan defensive OPSEC. Hide friendly critical information from enemy view using effective Electronic Protection (EP), cover, camouflage, concealment, decoys, cover stories, media control, etc.

b. Plan PSYOP in support of IO.

(1) ICW G-2, conduct PSYOP target analysis.

(2) PSYOP in support of IO.
1. Support deception operations.
2. Reduce enemy morale.
3. Encourage surrender.
4. Counter enemy propaganda.
5. Exploit ethnic and cultural differences.
6. Amplify effects of military operations.
7. Give alternatives to continued conflict.
8. Support US national policy in area of operations.
9. Reduce collateral damage in area of operations.

(3) Develop PSYOP:
1. Objectives.
2. Actions.
3. Targets.
4. Themes to stress and avoid.
5. Actors and players.
6. Desired end state.

(4) Plan PSYOP for offensive IO.
(a) Plan PSYOP against enemy operational level commander(s).
(b) Plan PSYOP against enemy control systems.
(c) Examples:
1. Attack enemy legitamacy and credibility.
2. Gain and sustain support to US position.
3. Influence loyalty of hostile forces.
4. Deter adversary powers and groups.
5. Promote cessation of hostilities.
6. Undermine confidence.

(5) Plan PSYOP for defensive IO.
(a) Influence enemy intelligence collection.
(b) Discourage/influence enemy use of IO.
(c) Examples:
1. Gain and maintain initiative.
2. Counter hostile propaganda.
3. Decrease impact of adversary operations.
4. Influence/discourage adversary operations.
5. Support maintenance of US/Allied coalitions.
6. Retaliation warnings.

c. Plan military deception in support of IO.

(1) Is the deception? Credible, verifiable, consistent, and simple.

(2) Military deception, in support of offensive IO.

(a) Achieve surprise.
(b) Preserve friendly forces, equipment, and installations from destruction.
(c) Minimize a physical advantage the enemy may have.
(d) Gain time.
(e) Cause commander to employ enemy forces in ways advantageous to friendly forces.
(f) Cause enemy commander to reveal strengths, dispositions, future intentions.
(g) Influence enemy intelligence collection and analysis systems.
(h) Condition enemy to friendly patterns of behavior that can be exploited.
(i) Cause enemy to waste combat power with inappropriate or delayed actions.

(3) Military deception in support of defensive IO.

(a) Conceal location/composition of friendly C2 nodes.

(b) Use military deception in support of OPSEC to help neutralize enemy Reconnaissance, Surveillance, and Target Acquisition (RSTA) efforts and feed enemy incorrect combat information.

(4) Do not portray conflicting military deception stories for offensive and defensive IO.

(5) Is the deception integrated with PSYOP and OPSEC?

(6) Plan to monitor feedback channels to observe enemy reactions.

d. Plan EW in support of IO.

(1) Plan Electronic Warfare Support (ES) in support of EW.

(a) Plan ES for offensive IO.
1. Develop combat information for immediate targeting of enemy emitters.
2. Develop combat information for rapid feedback of effectiveness of friendly offensive IO. Develop combat information for further analysis as SIGINT.

(b) Plan ES for defensive IO.
1. Develop combat information for immediate targeting of enemy ofensive IO capabilities.
2. Use ES to support Indications and Warning (I&W) of enemy attack and threat avoidance.

(2) Plan Electronic Attack (EA) in support of IO.

(a) Plan tactical jamming operations to cumulatively degrade enemy RSTA capability and C2.

(b) Plan electromagnetic deception in support of military deception operations to influence enemy RSTA efforts.

(c) Plan EA, using Anti-Radiation Munitions (ARM) to degrade, neutralize or destroy enemy personnel or equipment.
1. Establish/recommend high priority targets for use of destructive EA means.
2. Integrate ARMs with jamming, stealth, Precision Guided Munitions (PGM), and Direct Action (DA) missions, to counter enemy radar defenses.
3. Target enemy C2 nodes as a target set and in-depth.

(3) Plan Electronic Protection (EP) in support of IO.

(a) Plan EP for offensive IO.
1. Use ES for targeting enemy offensive IO capability.
2. Use COMSEC, TRANSEC and Signals Security (SIGSEC) to deny enemy information.

(b) Plan EP for C2-protect.
1. Coordinate with the G-6/Frequency Manager for development of the Restricted Frequency List (RFL).
2. Plan for EW Re-programming.

e. Plan destruction operations in support of IO.

(1) Develop IO-related High Value Target List (HVTL). Based on C4I nodal analysis.

(2) Plan destruction operations for offensive IO.

(a) Plan destruction against enemy command.
1. Target enemy commanders, staff, communications and intelligence production facilities, consistent with mission objectives.
2. Destruction is timed for when enemy most needs assets in decision cycle.

(b) Plan destruction against enemy control.
1. Target control nodes to degrade dissemination of information.
2. Target C2 nodes collectively as target sets.
3. Target C2 in depth.

(c) Plan to monitor destroyed/degraded C2 for evidence of reconstitution.

(3) Plan destruction operations for defensive IO.
(a) Integrate destruction with other IO elements.
(b) Destroy enemy offensive IO capability.
(c) Destroy enemy intelligence collection capability.

f. Plan Computer Network Operations (CNO) in support of IO.

(1) Plan CNO in support of offensive IO.
(a) Plan CNA against selected enemy networks; target C2, intelligence, logistics as required achieve mission objectives.
(b) ICW G-2, develop feedback mechanism for CNA operations.

(2) Plan CNO in support of defensive IO and Computer Network Defense (CND).
(a) Plan CNA against enemy offensive IO capabilities to preclude attacks on friendly information and C4I.
(b) ICW G-2, develop feedback mechanism for active defense operations.

g. Plan Defensive IO is support of IO.

(1) ICW G-6, conduct nodal analysis of friendly C2.
(a) Identify critical nodes.
(b) Identify vulnerable nodes.

(2) ICW G-2, conduct analysis of threat.

(3) Plan for:
(a) Computer Security (COMPUSEC).
(b) Information Security (INFOSEC).
1. Signal Security (SIGSEC).
2. Transmission Security (TRANSEC).
3. Communication Security (COMSEC).
4. Physical Security.
(c) Operations Security (OPSEC).

(4) ICW G-3/6 develop and coordinate Information Condition (INFOCON) levels.

h. Develop feedback mechanisms for command and control warfare effectiveness.

(1) ICW G-2/3/6, determine criteria for measures of effectiveness.
(2) Incorporate feedback into continuous planning cycle to modify or continue MAGTF IO efforts, as required.

i. Consolidate all IO plans into an IO synchronization matrix.

8. Provide input/develop IO input into plan/order. Because IO is multi-disciplined, it is found in various portions of the MAGTF Operations Order. See below.

APPENDIX 2 (SIGNALS INTELLIGENCE) TO ANNEX B (INTELLIGENCE)

APPENDIX 4 (TARGETING) TO ANNEX B (INTELLIGENCE)

APPENDIX 6 (INTELLIGENCE SUPPORT TO C2W) TO ANNEX B (INTELLIGENCE)

APPENDIX 3 (INFORMATION WARFARE) TO ANNEX C (OPERATIONS)
- TAB A – MILITARY DECEPTION
- TAB B – ELECTRONIC WARFARE
- TAB C – OPERATIONS SECURITY
- TAB D – PSYCHOLOGICAL OPERATIONS
- TAB E – PHYSICAL DESTRUCTION
- TAB F – COMPUTER NETWORK ATTACK
- TAB G – DEFENSIVE INFORMATION OPERATIONS

APPENDIX 1 (INFORMATION ASSURANCE) TO ANNEX K (COMMAND, CONTROL, AND COMMUNICATION, AND COMPUTER SYSTEMS)

ANNEX F (PUBLIC AFFAIRS)

ANNEX G (CIVIL AFFAIRS)

ANNEX S (SPECIAL TECHNICAL OPERATIONS)

ANNEX X
INFORMATION OPERATION PLANNING TOOLS

Information Operations Synchronization Matrix.

The IO synchronization matrix is commonly used during COA analysis to portray the time-phased aspects of the IO activities. The grid matrix shown below generally presents more detail than the following graphic matrix.

IO Synchronization Matrix					
Time Phase					
OPSEC					
PSYOP					
EW					
Physical Destruct					
Deception					
Civil Affairs					
Public Affairs					

Information Operations Planning Worksheet.

During COA development, IO planners can use a planning worksheet to develop IO tasks for each COA. One worksheet is completed for each IO objective; the cumulative worksheets are an outline for IO support for that COA. The IO Planning Worksheet helps tie together the staff products generated during scheme of maneuver development. They also focus task development in both offensive and defensive IO functions.

IO Planning Worksheet

Concept: _____
COA: _____
Objective: _____

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

Information Operation Execution Matrix.

The IO execution matrix converts the generalities of the synchronization matrix into specific taskings and requests to IO capable units. It is used during planning and execution.

IO Execution Matrix						
IO Task	Loca-tion	Means Employed / IO Element	Tasked Unit or System	Time	Assess-ment Method/ Means	Remarks
Execution/Coordination Instructions:						