

# Information Operations



## MAGTF Staff Training Program (MSTP)

U.S. Marine Corps  
July 2000

MSTP Pamphlet 3-0.4

# Information Operations

This pamphlet supports the academic curricula of the Marine Air Ground Task Force Staff Training Program (MSTP).

U.S. Marine Corps  
July 2000

UNITED STATES MARINE CORPS  
MSTP Center (C 467) MCCDC  
3300 Russell Road  
Quantico, Virginia 22134-5069

28 July 2000

**FOREWORD**

1. **PURPOSE.** MSTP Pamphlet 3-0.4 *Information Operations*, is designed to assist the staff officer in planning and executing information operations (IO).
2. **SCOPE.** This pamphlet provides an overview of IO doctrine, planning and execution techniques, and unique IO considerations. While the pamphlet is primarily focused at the Marine air-ground task force (MAGTF) level, this information is applicable to the Marine Corps component and major subordinate commands.
3. **SUPERSESSSION.** None.
4. **CHANGES.** Recommendations for improvements to this pamphlet are encouraged from commands as well as from individuals. The attached User Suggestion Form can be reproduced and forwarded to:

Commanding General (C 467)  
Training and Education Command  
3300 Russell Road  
Quantico, Virginia 22134-5001

Recommendations may also be submitted electronically to:  
[opso@mstp.quantico.usmc.mil](mailto:opso@mstp.quantico.usmc.mil)

5. **CERTIFICATION.** Reviewed and approved this date.

S.W. RAWSON  
Colonel, U.S. Marine Corps  
Director  
MAGTF Staff Training Program Center  
Marine Corps Combat Development Command  
Quantico, Virginia

Throughout this pamphlet, masculine nouns and pronouns are used for the sake of simplicity. Except where otherwise noted, these nouns and pronouns apply to either sex.

## USER SUGGESTION FORM

From:

To: Commanding General, Marine Corps Combat Development  
Command (C 54), 3300 Russell Road, Quantico, Virginia 22134-  
5001

1. In accordance with the Foreword, individuals are encouraged to submit suggestions concerning this Pamphlet directly to the above addressee

Page \_\_\_\_\_

Article/Paragraph No. \_\_\_\_\_

Line No. \_\_\_\_\_

Figure/Table No. \_\_\_\_\_

Nature of Change:

Add

Delete

Change

Correct

2. Proposed Text: (Verbatim, double-spaced; continue on additional pages as necessary.)

3. Justification/Source: (Need not be double-spaced.)

### NOTE:

1. Only one recommendation per page.
2. Locally reproduced forms may be used for e-mail submissions to:  
opso@mstp.quantico.usmc.mil

This page intentionally left blank.



This page intentionally left blank.

---

## Table of Contents

---

<b>Part I</b>	<b>Information Operations</b>	<b>1</b>
1001	Information Warfare	1
1002	Command and Control Warfare	2
1003	Information Operations and the Levels of War	2
1003a	Strategic Level of War	2
1003b	Operational Level of War	2
1003c	Tactical Level of War	3
1004	Fundamentals	3
1005	Information Operations Categories	4
1005a	Offensive Information Operations	5
1005b	Defensive Information Operations	5
1005c	Other Related Activities	7
1006	Elements of Information Operations	7
1006a	Operations Security	7
1006b	Psychological Operations	8
1006c	Military Deception	8
1006d	Electronic Warfare	8
1006e	Physical Destruction	9
1006f	Computer Network Attack	10
1006g	Public Affairs	10
1006h	Civil Affairs	10
1007	Intelligence Support	11
1008	Information Operations and the MAGTF	12
1008	Information Operations and the Marine Corps Component	13
<b>Part II</b>	<b>Planning</b>	<b>15</b>
2001	The Information Operations Cell	15
2002	The Marine Corps Planning Process	16
2002a	Mission Analysis	17
2002b	Course of Action Development	18
2002c	Course of Action War Game	20
2002d	Course of Action Comparison and Decision	20
2002e	Orders Development	21
2002f	Transition	21

<b>Part III</b>	<b>Execution</b>	23
3001	The Information Operations Cell and Current Operations	23
3002	The Information Operations Cell and Future Operations	24
3003	Signals Intelligence/EW Coordination Center	24
3004	Assessment	24
3005	Liaison	25
<b>Part IV</b>	<b>Unique Considerations</b>	27
4001	Deception	27
4002	Electronic Warfare	28
4003	Physical Destruction	30
4004	Psychological Operations	30
4005	Operations Security	31
4006	Computer Network Attack	33
4007	Information Assurance/Computer Network Defense	33
4008	Counter-Propaganda	34
4009	Counterdeception	35
4010	Counterintelligence	35
4011	Counterreconnaissance	36
4012	Special Information Operations	37
<b>Part V</b>	<b>Summary</b>	39
<b>Appendix A</b>	<b>Supporting Agencies</b>	41
<b>Appendix B</b>	<b>MAGTF Information Operations Assets</b>	51
<b>Appendix C</b>	<b>Operation Order Formats</b>	55
<b>Appendix D</b>	<b>Information Operations Planning Tools</b>	93
<b>Appendix E</b>	<b>Glossary</b>	97
<b>Appendix E</b>	<b>References</b>	101
<b>Figures</b>		
1-1	Information Operations Categories	4
1-2	Elements of Offensive Information Operations	5
1-3	Elements of Defensive Information Operations	6
2-1	Marine Corps Planning Process Steps	16

---

## Part I

# Information Operations

---

Information operations (IO) include 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—quite simply, it is dependent on mission, enemy, terrain and weather, troops and support available, time available. For example, 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 primitive means of communication, to facilitate civil affairs (CA), psychological operations (PSYOP), or tactical deception. Whatever the nature of the conflict, IO targets information or information systems to affect the information-based decisionmaking process. IO may, in fact, have its greatest impact as a deterrent in peace and during the initial stages of crisis. For example, IO can 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.

## **1001. 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. IW may be conducted to shape the battlespace and prepare the way for future operations. There is no other difference in scope or method between IW and IO.

## **1002. Command and Control Warfare**

Command and control warfare (C2W) is an application of IO/IW in military operations that specifically attacks enemy command and control (C2) capabilities while protecting friendly C2 capabilities. Destroying an enemy's ability to effectively command and control his forces has been, and continues to be, a very effective military technique. At the same time, protection of friendly C2 has proven to be just as important to successful military operations. In general, this pamphlet will use the more versatile term IO. It is a more inclusive term, and does not limit us in our concept of support to a narrow range of activities.

## **1003. 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.

### **a. 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 may 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.

### **b. 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, logistics, 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 the joint force to obtain and maintain the degree of information superiority required to quickly and decisively accomplish its mission.

### **c. Tactical Level of War**

IO 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.

## **1004. Fundamentals**

Following certain fundamentals is critical to successfully exploiting the significant potential that IO possesses in helping the MAGTF achieve tactical success. The following are the fundamentals of IO—

- *MAGTF IO must be synchronized and integrated with those of the higher and adjacent commands.* 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, 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.
- *The MAGTF commander's intent and concept of operations determine IO targets.* 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. C2 systems are a substantial target for IO. Friendly systems critical to the friendly forces should be protected.
- *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.

A 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 decisionmaking 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 opponent’s information. IO can slow or halt entirely the flow of information; it can change the accuracy or truthfulness of the data within the information system. The decisionmaking process is dependent upon information—poor information prevents the enemy from developing accurate situation awareness and slows down his decisionmaking process. The enemy’s plan, decide, execute, and assess cycle can no longer compete with the friendly tempo. Overwhelming operational tempo is generated, facilitating success.

### 1005. Information Operations Categories

There are two mutually supporting categories of IO. Common links between the two aspects—offense and defense—include the information systems involved and the dependence upon information to plan operations, deploy forces, and execute missions. See Figure 1-1.

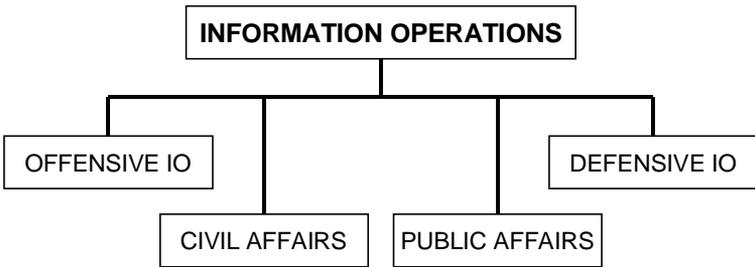


Figure 1-1. Information operations categories.

## a. Offensive Information Operations

Offensive IO involves the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decisionmakers and their information and information systems. These capabilities and activities include, but are not limited to: operations security (OPSEC), military deception, PSYOP, electronic warfare (EW), physical attack/destruction, and computer network attack (CNA). The human decisionmaking process is the ultimate target for offensive IO. Offensive IO objectives must be clearly established, 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. When employed as an integrating strategy, IO weaves together related capabilities and activities toward satisfying a stated objective. Offensive IO distorts 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 produces a dramatic impact on the enemy decisionmaking process. See Figure 1-2.

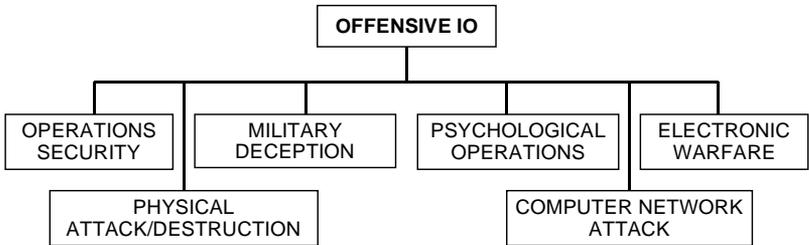


Figure 1-2. Elements of offensive information operations.

## b. 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, counterdeception, counterpropaganda, counterintelligence (CI), and EW. See Figure 1-3.

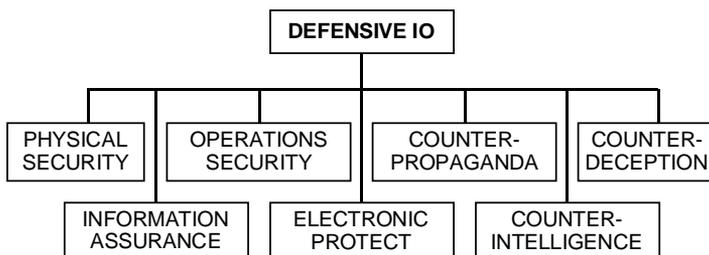


Figure 1-3. Elements of defensive information operations.

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 ensures the necessary protection and defense of information and information systems upon which the MAGTF depends to conduct operations and achieve objectives. Four interrelated processes comprise defensive IO—

- **Information Environment Protection.** Defining MAGTF needs and 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.

### **c. Other Related Activities**

Related activities are operations that are neither offensive nor defensive IO in nature but must be coordinated with all other IO efforts. Such activities include public affairs (PA) and CA.

## **1006. Elements of Information Operations**

IO is composed of distinct 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.

### **a. 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 command decisions that could prove devastating to the enemy force. 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.

## **b. Psychological Operations**

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 encourages enemy forces to defect, desert, flee, or surrender. At the tactical level, PSYOP include the use of loudspeakers and other means to promote fear or dissension in enemy ranks. PSYOP may support military deception operations.

## **c. Military Deception**

Military deception targets enemy decisionmakers by deceiving their intelligence collection, analysis and dissemination systems. This deception requires a thorough knowledge of opponents and their decisionmaking processes. Military deception is focused on desired behavior, not simply to mislead. The purpose is to cause enemy commanders to form inaccurate impressions about friendly force capabilities or intentions by feeding inaccurate information through their intelligence collection assets. The goal is to cause the enemy commander 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.

## **d. Electronic Warfare**

EW is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions of EW are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). All three contribute to both offensive and defensive IO.

- **Electronic Attack.** EA is concerned with denying an enemy commander the use of the electromagnetic spectrum to effectively command and control operating forces. Whether through jamming, electromagnetic deception, or destruction of C2 nodes with directed energy weapons or anti-radiation missiles, EA has a major role to play in almost all C2 attack operations. The decision to employ EA should be based not only on overall operation objectives, but also on the potential impact on friendly operations and the effects of possible enemy responses.
- **Electronic Protection.** EP is protecting the use of the electronic spectrum to command and control friendly forces. It involves such action as self-protection jamming and emission control taken to protect friendly use of the electronic spectrum. It minimizes the effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability. Coordination of the use of the electromagnetic spectrum by friendly forces through the joint restricted frequency list (JRFL) is a means of preventing interference between friendly electronic emissions. EP is routinely conducted during peacetime as well as periods of crisis or conflict.
- **Electronic Warfare Support.** ES contributes to situational awareness in the area of operations by detecting, identifying, and locating sources of intentional or unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. ES can provide real-time information to locate and identify C2 nodes and supporting early warning and offensive systems. Used to produce signals intelligence (SIGINT), ES can provide timely intelligence about an enemy's C2 capabilities and limitations that can be used to update previously known information about the enemy's C2 systems. This updated information can be used to plan offensive IO, provide battle damage assessment of IO attacks, and feedback on the effectiveness of the overall IO plan.

## e. Physical Destruction

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 that 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 reattack if analysis determines that they are still critical in the overall IO/IW effort. To preclude reconstruction, physical destruction should usually be timed for just before the enemy needs a certain C2 capability.

## **f. 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 (Joint Pub 1-02). Some of the tools and expertise required are readily obtained from the Internet. The widespread availability of attack methods combined with the possibility of working from remote locations makes CNA a significant potential threat. The MAGTF will normally not have an offensive CNA capability, but it must be both aware of joint capabilities and prepared to defend against the CNA threat.

## **g. 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) (Joint Pub 1-02). These activities expedite the flow of accurate and timely information to internal and external audiences. As an 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.

## **h. Civil Affairs**

CA 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. CA may include performance by military forces of activities and functions normally the responsibility of local government (Joint Pub 1-02). CA and PSYOP are mutually supportive within

civil-military operations. CA 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.

## **1007. 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 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, and cultural influences on decisionmakers.
- An understanding of the enemy's decisionmaking process.
- An intimate knowledge of the biographical background of key enemy decisionmakers, communicators, and their advisors, to include biographical sketches, career histories, motivating factors, and leadership styles.
- Geographic and atmospheric influence on enemy and friendly operations.
- Assessment of potential enemy capability and intent to attack or exploit friendly information and information systems.

Once IO activities have commenced, the role of intelligence continues. 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. 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.

## **1008. Information Operations and the MAGTF**

The primary focus of MAGTF IO activities will be at the tactical level 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.

Since MAGTFs will almost invariably fight as a part of a larger joint force, their offensive and defensive IO efforts will support and be coordinated with the IO plans of the joint force and adjacent commands. The JFC will have standing IO procedures and perhaps a standing IO plan based on 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 and integrate into the JFC IO plan; in turn, the major subordinate commands will need to develop supporting IO plans appropriate for their level of command.

## 1009. Information Operations and the Marine Corps Component

The Marine Corps component is responsible for setting the conditions and creating the environment for successful 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 data bases in conjunction with the component intelligence staff
- Developing component IO policy as needed consistent with the JFC's IO policies
- 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*.

This page intentionally left blank.

---

## Part II

# 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 of the higher headquarters, and integrated into the unit operation plan. The IO cell and the Marine Corps Planning Process (MCP) are two important tools in successful IO planning.

### **2001. The Information Operations Cell**

The IO cell is a small 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 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, and 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, augmentation from supporting IO activities, and representatives from staff elements and appropriate warfighting function/subject matter experts. Supporting IO units and agencies could include such organizations as radio battalion, 4<sup>th</sup> Civil Affairs Group (CAG), the Fleet Information Warfare Center (FIWC), the Joint Information Operations Center (JIOC), Joint Warfare Analysis Center

(JWAC), or the Land Information Warfare Agency (LIWA). Care should be taken to tailor the size and structure of the cell to meet the needs of 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.

## 2002. The Marine Corps Planning Process

The MCPP supports decisionmaking 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 C2, the MCPP recognizes the commander's central role as the decisionmaker. 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.

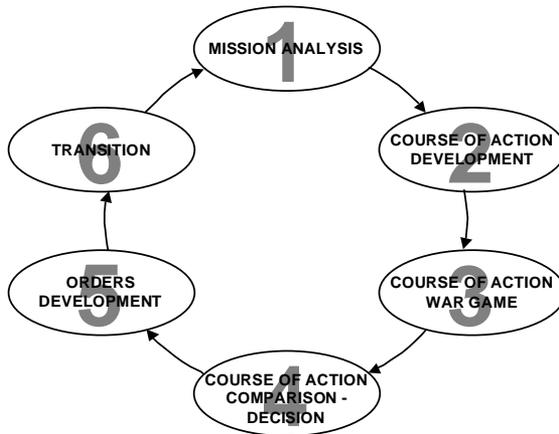


Figure 2-1. Marine Corps Planning Process steps.

The MCPP organizes the planning process into six manageable, logical steps (see figure 2-1). It establishes procedures for analyzing a mission, developing and war gaming 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 through the IO cell with all six warfighting functions and the higher, adjacent, and subordinate commands.

## **a. 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 dissected to extract IO planning guidance such as constraints, restrictions, and planning factors. This guidance establishes the boundaries for IO planning, identify target limitations based on policy, 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, IO 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 (described in detail in Part I) are developed or requested. Enemy IO strengths and vulnerabilities are identified for additional examination and possible exploitation by friendly IO. 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.

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. Once completed, it can eventually be included in the operations order with minimal adjustments.

The IO cell must participate in the MAGTF's planning activities and constantly coordinate its planning efforts with those of the MAGTF future operations. 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 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 be potential IO targets.

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.

## **b. 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 will graphically display friendly IO assets and enemy C2 links and nodes to allow the planners to see the current and projected locations of friendly and enemy forces. In coordination with the Red Cell, 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 scrutiny. 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 a generic 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.

### **c. 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 generic 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.

Planning tools and products tailored to IO requirements are contained in Appendix D.

#### **d. 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.

### **e. 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 IO generic 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, Appendices 1-5, IO can also be addressed in Annex B, Intelligence; Annex S, Special Technical Operations, and Annex U, Information Management. See Appendix C for additional information on the preparation of IO related material for inclusion in operation orders. 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.

### **f. 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.

This page intentionally left blank.

---

## Part III

# Execution

---

Effective employment of IO depends on the ability of the MAGTF to monitor execution of the plan and adjust operations to meet the changing situation. The IO cell will continue to play a central role for the MAGTF in the management of the unit IO plan.

### **3001. The Information Operations Cell and Current Operations**

The IO cell is part of and works for the G-3. It assists the MAGTF current operations section in the execution of the MAGTF operations order. The IO cell monitors the implementation of the IO plan, adjusting as required. The IO cell may be represented in both in the current operations watch section and the MAGTF targeting board to ensure the IO plan is executed properly.

IO personnel may be part of the current operations watch section. The IO cell members monitor reports from IO-capable units to ensure that IO targets are attacked in accordance with the IO plan. They also ensure that assessment of the status of IO targets, and that analysis is conducted to determine the necessity for restrike and adjustment of attack methods.

The IO cell helps the MAGTF targeting board determine the best methods of attacking enemy targets. IO cell members provide subject matter expertise to the targeting board and ensure that IO considerations are incorporated based on the concept of operations. As necessary, they may represent the MAGTF on higher headquarters targeting boards. Additionally, the IO cell can conduct reactive IO targeting by identifying targets of opportunity, redirecting IO assets, and coordinating attack of those targets. The IO cell will also coordinate MAGTF IO activities with those of the JFC. Since IO may be conducted before actual combat operations, the IO cell should have the communications connectivity, either through the COC or separately, to coordinate changing IO requirements.

## **3002. The Information Operations Cell and Future Operations**

The IO cell ensures that the current IO actions are given to the future operations cell to be used into their planning efforts. Future operations focuses on changes to the MAGTF or major subordinate command missions; develops branch plans and sequels; and recommends potential CCIRs. Future operations coordinates with intelligence collection and the targeting process to shape the next battle. To conduct IO planning, future operations relies upon the IO cell. These individuals will assess current IO shaping actions and the progress toward the commander's decisive actions, monitor the status of IO forces and actions, and provide future operations information on the effectiveness of IO events for continued planning.

## **3003. Signals Intelligence/EW Coordination Center**

The signals intelligence/electronic warfare coordination center (S/EWCC) is the focal point for all coordination required between the SIGINT and EW efforts within a MAGTF. It coordinates the planning, execution, and evaluation of all SIGINT and EW operations. It is composed of representatives from the G-2 (the SIGINT/ground EW officer), G-3 (the EW officer), the G-6 (the frequency coordinator), and other MAGTF EW capable organizations (Marine tactical electronic warfare squadron [VMAQ], radio battalion, etc). It meets (usually daily) to deconflict SIGINT and EW operations and to ensure that these operations do not interfere with friendly communications. IO cell participates in the S/EWCC deliberations to ensure that the EW portion of the IO plan is being executed properly and to adjust the IO plan if the S/EWCC determines that it is necessary.

## **3004. Assessment**

Feedback and monitoring of ongoing IO actions is critical to the success of IO. Without such information, resources can easily be wasted on ineffective activities that could even be detrimental to the MAGTF mission. Appropriate assessment procedures to support IO should be developed and established. An assessment plan should be developed as part of the overall IO plan. This plan should answer the following questions:

- What intelligence assets will be tasked to monitor IO targets?
- What targets will be monitored and for which indicators?
- What are the reporting requirements?
- What are the feedback taskings to other IO capable organizations participating in the execution of the IO plan?

As the reports on IO actions are received, the IO cell analyzes the results and determines the degree to which specific IO actions are successful. It uses the measures of effectiveness established as part of the assessment plan. Based on these criteria, the IO cell determines if continued attack with a specific IO action is necessary or advisable. The IO cell can add additional IO resources, or switch to a different IO tactic. For example, if the requirement is to halt communications along a specific link and EW has been ineffective, then physical destruction might be recommended. It can even recommend to current operations that a non-IO action be used. Once success has been achieved, the IO cell can direct an end to the IO activity and redirect resources elsewhere.

### **3005. Liaison**

The IO cell is an important link between the MAGTF and other IO resources. Many of the IO assets that support the command's mission will be external to the MAGTF, and the IO cell must synchronize the efforts of these supporting organizations with those of the MAGTF. If available, liaison officers from these organizations should be integrated into the IO cell planning and execution. The size, structure, and planning methods used by these organizations vary widely. These IO organizations will control the IO activities of their own forces, but will be reporting to and receiving requests for support from the IO cell. The end result should be an integrated IO plan controlled and executed through the IO cell.

This page intentionally left blank.

---

## Part IV

# Unique Considerations

---

IO is not a risk- or cost-free activity. Whenever a unit uses IO, it must evaluate the degree of integration or conflict with the higher headquarters IO plan, the amount of time and resources required, the risks that an IO failure might impose, the legal constraints, and the unintended consequences of an IO action. For example, IO often requires a longer lead-time to effect the enemy than other operations, and the impact of IO on the enemy may not be readily apparent at the time of execution. A sophisticated assessment effort must be conducted to determine the actual impact and reduce uncertainty for the MAGTF commander.

### **4001. Deception**

A convincing deception may require significant resources to be believable. Good deceptions can use false radio traffic, actual movement of meaningful numbers of personnel, equipment, and supplies, air and ground strikes against misleading targets, physical mockups, and pre-recorded sounds—all supporting a believable plan. These efforts can consume an enormous amount of resources.

In deception, timing is everything. Time must be taken into account for the deception to occur, the enemy's intelligence system to collect, analyze, and report, for the enemy decisionmaker to react, and for the friendly intelligence system to detect the action resulting from the enemy's decision.

The objective of the deception must be to cause the decisionmaker to take (or not to take) specific actions, not just to believe certain things. The deception plan must identify and target the enemy decisionmaker capable of taking the desired actions. The enemy's intelligence system is not normally the target, but only the conduit used to get selected information to the decisionmaker.

The deception plan should be fully integrated into the actual operation. It should be a plausible COA and “fit” the rest of the operations plan. It should not stand out as an anomaly and alert the enemy prematurely. The MAGTF deception plan must nest within any deception plan created by the higher headquarters. The plan should depict a variety of indicators from multiple sources. This will lend credibility to the story, permit the enemy to verify the story, and provide the targeted enemy decisionmaker with more opportunities to conclude the deception is real.

Military deception operations can be resource intensive. The enemy must be able to verify the veracity of the deception story through multiple channels. The deception plan must take into account all of the enemy’s intelligence sources. The story must be made available through all or many of those sources, each providing the target with a small piece of the deception story. Providing the resources and units to generate believable story indicators can conflict with other operational requirements.

Military deception requires accurate intelligence. The MAGTF intelligence assets must be able to identify appropriate deception targets, assist in developing a credible story with indicators that the enemy is capable of collecting with his intelligence assets, and to assess the extent to which the enemy has been deceived. If the deception plan is such that intelligence cannot corroborate success, the plan may not be worth implementing.

Deception operations should be closely coordinated with the PSYOP campaign and CA. If not, once the actual operation has been revealed, the relationships with the civilian population or with host-nation military authorities may be inadvertently undermined once they realize that their allies deceived them as well. However, military deception will not use PA as a conduit for false information. Although the deception will plant misleading indicators for the enemy to collect and analyze, it will not use U.S. spokesmen to lie or provide disinformation to either internal or external audiences.

## **4002. Electronic Warfare**

The three sub-divisions of EW (EA, EP, and ES) must be integrated with each other and with the rest of the operations plan. EA personnel have good idea of enemy SIGINT collection capabilities, and can alert CI and OPSEC specialists. Jamming can be synchronized with SIGINT to force the enemy

to communicate unencrypted to facilitate intelligence collection. The benefits of preventing the enemy from communicating by physical destruction and EA must both be weighed against the possible intelligence lost by not monitoring those communications. The S/EWCC is the ideal mechanism to enable the commander to resolve these issues.

In peacetime, government organizations, international treaties, and conventions control the use of the electromagnetic spectrum. EW used in support of military operations other than war is normally restricted to actions that do not violate the peacetime use of the spectrum. Under peacetime ROE, the only exception is when action is necessary to protect friendly forces. During military operations that involve hostilities, control of the electromagnetic spectrum will often be contested and the full range of EW actions may be available. The appropriate type and level of EW actions depend on the threat, the extent to which the enemy is reliant on the electromagnetic spectrum, and the objectives of the operation.

EW activities must always be synchronized with EW activities of the higher headquarters. The JTF coordinates the use of the electromagnetic spectrum with planned EW operations through the JRFL, identifying protected, guarded, and taboo frequencies.

### **Joint Pub 1-02**

**Protected frequencies:** Friendly frequencies.

**Guarded frequencies:** Enemy frequencies from which SIGINT is being derived.

**Taboo frequencies:** Critical friendly frequencies that must never be jammed or interfered.

The JFC's EW staff plans and assesses EW operations, assists in emissions control and command, control, and communications countermeasures strategy, and coordinates EW and psychological transmissions. This staff ensures coordination among EW and other IO and communications support activities for maximum effect and to reduce electronic fratricide. Such coordination is necessary for the effective exchange of information, to eliminate undesirable duplication of effort, and to provide mutual support.

### **4003. Physical Destruction**

As part of IO, physical destruction is synchronized with the maneuver plan and tied to critical events and decision points. “Hard kill” weapons are usually preferred to attack coastal surveillance and integrated air defense systems, enemy offensive IO capabilities, and selected C2 nodes and facilities. The employment of physical destruction (as with EW) and the prevention of the enemy use of any particular communication link or node should be weighed against the possible loss of intelligence that may have been collected from that communication link. ROE may also impact on the use of physical destruction. For example, if physically attacking the target might cause collateral civilian casualties, the ROE might dictate that some other IO is used. Physical destruction can have an immediate result, but it is often difficult to discern the impact on the decisionmaking process (i.e., a communication facility may be observed as destroyed, but the enemy may shift to an alternate command post or use a different communication means). Timing of physical attacks is important to not allow the enemy to restore the destroyed capability.

### **4004. Psychological Operations**

As with most IO operations, MAGTF PSYOP must be coordinated with the JFC. The joint force PSYOP officer ensures continuity of psychological objectives, themes to stress and avoid, and target audiences by all components. Dedicated PSYOP personnel with adequate language and area expertise and resources are always in short supply. Due to this scarcity and the requirement for a consistent PSYOP message, a joint psychological operations task force (JPOTF) is normally formed to coordinate execution of the JFC’s PSYOP plan. When a JPOTF is established, tactical PSYOP forces are usually placed in direct support of maneuver elements. Dissemination forces operate in general support of the JFC with tactical control by the JPOTF commander. Multipurpose assets that are primarily PSYOP platforms, such as COMMANDO SOLO (EC-130 aircraft equipped for airborne broadcasting of radio and television signals), remain under the operational control of the component commander while under tactical control of the JPOTF commander. Task-organized PSYOP teams are available to support smaller operations when a JPOTF is not required. Most PSYOP products will be developed by the JPOTF.

The MAGTF should consider and plan for the early conduct of PSYOP and, if required, use of host-nation resources and non-PSYOP military assets for media production and dissemination; e.g., use of navy ship's printing facilities for production of PSYOP products. Use host-nation and U.S. Country Teams (the senior, in-country, US coordinating and supervising body, headed by the Chief of the US diplomatic mission) to gain local support. Ensure comprehensive coordination of plans with those staff elements or agencies that generate information, such as the public affairs officer, so all information activities are consistent.

The most numerous and generally useful means to conduct PSYOP are open sources of information. These means should be accessible to or observable by the target groups. However, care should be taken when using non-PSYOP outlets to disseminate the PSYOP message. There may be legal or ROE restrictions that apply to the use of civilian communications by the military. Under the UN Convention on Law of the Sea, PSYOP broadcasts from the sea may constitute unauthorized broadcasting. In any event, the MAGTF should establish a PSYOP reporting system to provide relevant information to PSYOP planners about the apparent impact of friendly PSYOP activities and any anticipated changes to ongoing activities.

## **4005. Operations Security**

To be successful, OPSEC must be integrated early into planning. Early planning will reduce the chances of the MAGTF revealing indicators of its intentions, force the enemy to make faulty decisions based upon insufficient information, and delay their decisionmaking process due to a lack of information.

The OPSEC process consists of five actions: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate OPSEC measures. First, the MAGTF seeks to identify the questions that it believes the enemy will ask about friendly intentions, capabilities, and activities—that is essential elements of friendly information (EEFI). These questions are further refined to identify the critical information vitally to the enemy. Identifying and protecting this subset of EEFI is the focus of the OPSEC process. Denying all information about a friendly operation or activity is seldom cost effective or realistic.

An **EEFI** is defined in Joint Pub 1-02 as:

Key questions likely to be asked by enemy officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness.

**Critical information** is defined in Joint Pub 1-02 as:

Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

Then, the OPSEC planners research and analyze the enemy's capabilities. The planners then identify the friendly OPSEC vulnerabilities by determining indicators that could reveal critical information and then comparing those indicators with the enemy's intelligence collection capabilities. Next, they conduct a risk assessment, comparing the estimated cost of each possible OPSEC measure to the potential harmful effects should the enemy succeed in acquiring the critical information. Finally, the OPSEC measures are implemented and the reaction of the enemy to the measures is monitored to determine their effectiveness.

CI support is an integral part of successful OPSEC. PSYOP, PA, military deception, EW, and targeting personnel also work closely with OPSEC planners to mutually support their respective efforts. The OPSEC process may also identify for attack enemy collection systems to hinder the enemy's ability to collect critical information.

OPSEC planning is a continuous process. During the execution phase of the operation, feedback on the success or failure of OPSEC measures is evaluation and the OPSEC plan is modified accordingly. The termination of OPSEC measures must be addressed in the OPSEC plan to minimize the adverse cost and impact, and to prevent future enemies from developing countermeasures to successful OPSEC measures.

## 4006. Computer Network Attack

Offensive CNA activities will probably be conducted by national-level organizations or other Service components. While CNA may be an appropriate IO tool to attack or degrade enemy C2 nodes and links, there are international legal restrictions that may apply to use of CNA against international civil aviation and financial institutions. ROE must be closely examined and clearly defined. Additional guidance on CNA is available in the classified appendix (“Supplemental Information Operations Guidance”) to Joint Pub 3-13, issued separately.

## 4007. Information Assurance/Computer Network Defense

Information assurance protects friendly information. For defense against enemy CNA actions, the MAGTF analyzes its information systems to determine its vulnerabilities, considering both military and nonmilitary systems, and coordinates the efforts to reduce risks inherent in nonmilitary systems.

**Information assurance** is defined in Joint Pub 1-02 as:

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

A program to reduce risk should be implemented which would evaluate the value of the information that may be compromised or lost if the system is breached versus the resources available for protection and defense. Protection should apply to any information medium or form, including fax machines, storage media, video and imagery, and computers and the links that connect them. The MAGTF can then take defensive measures to reduce its own vulnerabilities to enemy CNA actions.

The first step to defeating a network intruder is the preparation of defenses. Avoid permitting the friendly information systems to be detected. If detected, it should appear insignificant and not worth attacking. Network defenses should be layered but they can only buy time and not full protection. Given enough time and a communications link, an intruder can eventually break into any computer network and acquire information that could be detrimental to friendly operations. The second step to defeating intruders is the detection of the intrusion attempt (where, when) and the capability being used to perform the intrusion. The third step is the development of contingency actions to defeat the intrusion threat based on time and planning considerations established by the MAGTF commander. This allows the MAGTF to choose when and where to degrade, defeat, deceive, or possibly destroy the threat once it is detected. Only through a comprehensive plan to defend against hostile intrusion can a network truly be protected. The MAGTF information management officer (IMO) must work closely with the staff to provide adequate protection to command databases and critical data networks.

#### **4008. Counter-Propaganda**

Counter-propaganda is the planning and conducting of operations (preventive actions, counteractions, and rumor control) to negate enemy propaganda efforts or mitigate their effects. Such operations require intelligence and rear units to continuously monitor the civilian and military population in the rear areas to detect enemy propaganda efforts. The MAGTF should establish a propaganda reporting system to provide relevant information to planners about identified enemy propaganda activity. Counteractions should be planned to limit the effects of an enemy's potential propaganda effort before, during, and after U.S. military combat operations. Preventive action informs U.S. and coalition forces and local populations and exposes them to the existence and nature of enemy propaganda. Counteraction reduces or neutralizes the effects of the enemy propaganda, usually by stressing the clear goals of the U.S. Rumor control acknowledges the existence of specific rumors, furnished factual information, and tries to educate the populace to discount all rumors as untrustworthy.

## **4009. Counterdeception**

Counterdeception supports defensive IO by negating, neutralizing, or diminishing the effects of—or gaining an advantage from—a foreign deception operation. Activities contributing to awareness of enemy posture and intent also serve to identify enemy attempts to deceive friendly forces. Identifying enemy deception efforts are difficult, given that a good deception plan attempts to reinforce existing judgements or biases. Intelligence analysts must be aware of the possibility of deception on the part of the enemy and ensure that their analysis constantly reevaluates the situation in light of new information.

## **4010. Counterintelligence**

CI activities contribute to defensive IO by providing information and conducting activities to protect and defend friendly information and information systems against espionage, sabotage, subversion, or terrorist activities. CI assets are normally employed in general support to provide area coverage and disrupt the enemy's efforts to collect information concerning MAGTF units, infiltrate enemy agents, and conduct sabotage and terrorist activities. Emphasis is usually placed on force protection and rear area security operations. CI targets include personalities, organizations, and installations of intelligence or CI interest that should be seized, exploited, or protected. CI operations must be coordinated with and approved by the JFC CI coordinating authority. The JFC establishes areas of responsibility for CI operations; integrates, produces and disseminates CI products; and coordinates and obtains intelligence and CI support from national agencies and then disseminates this information. Sensitive CI information that may reveal methods and sources will be properly protected and reported via designated CI channels. CI personnel should coordinate CI activities with the staff judge advocate to ensure compliance with law and regulation prior to execution. Some CI operations may be restricted by existing Status of Forces Agreements with the HN. Where appropriate, the staff judge advocate should be part of the planning process. Special funds for conducting CI operations and intelligence collection activities by CI personnel will be made available by Headquarters Marine Corps.

## 4011. Counterreconnaissance

Counterreconnaissance includes all measures taken to prevent enemy observation of a force, area, or place. The counterreconnaissance force is task-organized based on the commander's guidance, intelligence collection requirements, and the estimate of the enemy reconnaissance force. Because of the importance of winning the counterreconnaissance battle, a large counterreconnaissance force is often required. U.S. Army doctrine indicates that this force may be up to one-third of the entire unit. EW may be used to suppress enemy reconnaissance reporting, deception to mislead enemy reconnaissance, and physical attack to destroy reconnaissance units.

Intelligence is critical for the MAGTF to target, destroy, or suppress the enemy's reconnaissance and surveillance assets. The key to counterreconnaissance intelligence support is finding enemy reconnaissance units before they can discover friendly positions and report back. Using situation and event templates that show enemy reconnaissance movement, intelligence can visualize how the enemy may be expected to conduct reconnaissance operations.

Enemy reconnaissance elements will most likely operate in small elements that can traverse almost any kind of terrain and may not use obvious avenues of approach. The enemy reconnaissance mission is to seek and report information, not to fight, so enemy reconnaissance will use routes that have plenty of concealment and cover. As a general rule, the more concealment or protection a route provides, the more likely it will be used by reconnaissance elements.

A careful study of the effects of weather and terrain on enemy reconnaissance will determine at what point the enemy can observe friendly positions. Usually, this is a function of line of sight and visibility in the area of operations. These limits are then compared with the enemy's known reconnaissance observation capabilities (such as infrared, thermal, light enhancement, and telescopic). As described in FM 34-2-1, this analysis will identify a limit of enemy advance for reconnaissance units. The counterreconnaissance effort must prevent the enemy from going beyond this limit to where the enemy can observe friendly positions. The MAGTF can then concentrate its counterreconnaissance attention on these named areas to detect enemy reconnaissance activity.

## **4012. Special Information Operations**

Special information operations are information operations that, by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the U.S., require a special review and approval process. These operations can be difficult to plan because the security requirements and the controlled access prevent easy coordination. Refer to the classified annex to Joint Pub 3-1.

This page intentionally left blank.

---

## Part V

# Summary

---

The doctrine of maneuver warfare requires that the enemies weaknesses must be identified and attacked through a series of rapid, focused, and unexpected actions which create a rapidly deteriorating situation with which the enemy cannot cope. The objective is the destruction of the enemy's moral, mental, and physical cohesion. IO focuses on the vulnerabilities and opportunities presented by the increasing dependence of the U.S. and potential adversaries on information and information systems. Systems that support the decisionmaking process can be made vulnerable to IO attack. The opportunity for the MAGTF commander lies in the successful exploitation of those vulnerabilities with tools other than just physical attack.

IO is an integrated strategy that facilitates the warfighting functions of C2, fires, maneuver, logistics, intelligence, and force protection and enables the MAGTF commander to accomplish the mission. It does not function well when conducted independently. From the initial stages of mission analysis through to the conclusion of the operation and the redeployment of forces, IO should be integrated into all aspects of the plan. MAGTF IO should fully support higher headquarters IO, as well as take advantage of those IO capabilities resident within higher and adjacent forces.

A fully functional IO cell is critical to successful IO. The IO cell should be formed early in the planning process with adequate personnel, expertise, and intelligence support. The IO cell integrates the broad range of potential IO action and activities (higher headquarters and organic) into the MAGTF plan and ensures IO support. The integration of IO will require planning and coordination among the staff, major subordinate commands, and higher headquarters. During execution, the cell monitors and assesses the effectiveness of IO on the enemy's decisionmaking process and adjusts accordingly.

IO should be treated as a single activity with both offensive and defensive applications. Many different capabilities and activities must be integrated to

achieve a coherent IO plan. OPSEC, PSYOP, EW, physical destruction, deception, CA, and PA should be coordinated to attack the enemy's weaknesses to support the concept of operations. Selection and employment of specific offensive IO capabilities against the enemy must be appropriate to the situation and consistent with the MAGTF's objectives. Defensive IO should be integrated into all military operations to provide a defense in depth and ensure the execution of the MAGTF operation. While there are some unique IO planning and execution considerations, the greatest challenge of IO is assessment. Effective assessment is only possible with continuous close coordination between IO, operations, and intelligence personnel.

MCDP 1 stresses that "while striving ourselves to overcome the effects of friction, we must attempt at the same time to raise our enemy's friction to a level that weakens his ability to fight." IO can be a means to overcome friction and to increase that of the enemy, but only if the MAGTF is organized and trained to use IO effectively.

---

## Appendix A

# Supporting Agencies

---

### **A-1. National Infrastructure Protection Center**

The National Infrastructure Protection Center (NIPC) was established in February 1998. Its mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures include telecommunications, energy, banking and finance, water systems, government operations, and emergency services. The mission of the NIPC is both a national security and law enforcement effort to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and "cyber," that threaten or target critical infrastructures. The NIPC's job is not simply to investigate and respond to attacks after they occur, but to learn about preventing them. The NIPC provides a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC provides the principal means for facilitating and coordinating the Federal Government's resources to an incident, mitigating attack.

### **A-2. National Counter Intelligence Center**

The National Counter Intelligence Center (NACIC) coordinates the U.S. Government's effort to identify and counter foreign intelligence threats to U.S. national and economic security. Operating under the auspices of the National Security Council, the NACIC draws its staffing from CI and security professionals from the Federal Bureau of Investigation, Central Intelligence Agency, Defense Intelligence Agency, National Security Agency (NSA), the Office of Secretary of Defense, the military Services, and the Departments of State and Energy. With the creation of the NACIC, CI information should reach the security countermeasures community on a more frequent and timely basis.

### **A-3. United States Information Agency**

The United States Information Agency (USIA) was an independent foreign affairs agency within the executive branch of the U.S. government until October 1999, when it was integrated into the Department of State. USIA maintains 190 posts in 142 countries, and overseas is known as the U.S. Information Service.

The mission of USIA is to understand, inform, and influence foreign publics in promotion of the national interest, and to broaden the dialogue between Americans and U.S. institutions, and their counterparts abroad. USIA explains and supports American foreign policy and promotes U.S. national interests through a wide range of overseas information programs. The agency promotes mutual understanding between the United States and other nations by conducting educational and cultural activities. Specifically, USIA works—

- To explain and advocate U.S. policies in terms that are credible and meaningful in foreign cultures.
- To provide information about the official policies of the United States, and about the people, values, and institutions which influence those policies.
- To bring the benefits of international engagement to American citizens and institutions by helping them build strong long-term relationships with their counterparts overseas.
- To advise the President and U.S. government policy-makers on the ways in which foreign attitudes will have a direct bearing on the effectiveness of U.S. policies.

USIA operates the U.S. government's programs of educational and cultural exchange. The International Broadcasting Act of 1994 established a Broadcasting Board of Governors to oversee USIA's Voice of America, Radio and TV Martí, and WORLDNET Television, as well as two surrogate international broadcast services—Radio Free Europe/Radio Liberty and the new Radio Free Asia. Unlike USIA's other federally funded broadcast services, Radio Free Europe/Radio Liberty, a non-profit private corporation, and Radio Free Asia receive funding through grants from the USIA's Broadcasting Board of Governors.

## **A-4. National Security Agency**

The NSA is a unified organization structured to provide SIGINT mission for the U.S. and to insure secure communications systems for all departments and agencies of the U.S. Government. NSA produces and disseminates SIGINT in accordance with the objectives, requirements and priorities established by the Director of Central Intelligence.

The Director exercises SIGINT operational control over SIGINT activities of the U.S. Government to respond most effectively to military and other SIGINT requirements. In the case of mobile military SIGINT platforms, the Director shall state movement requirements through appropriate channels to the military commanders, which retain responsibility for operational command of the vehicle. Subject to the authority, direction and control of the Secretary of Defense, the Director, National Security Agency/Chief, Central Security Service, is specifically delegated authority to—

- Exercise SIGINT operational control over SIGINT activities of the U.S.
- Issue directives to any operating elements such instructions and orders necessary to carry out his responsibilities and functions
- Have direct access to, and direct communications with, any element of the U.S. Government performing SIGINT functions.
- Adjust as required, through the Service cryptologic organizations, personnel resources under SIGINT operational control.
- Centralize or consolidate SIGINT operations for which he is responsible to the extent desirable, consistent with efficiency, economy, effectiveness, and support to field commanders.

The NSA information security (INFOSEC) mission provides leadership, products, and services to protect classified and unclassified national security systems against exploitation due to interception, unauthorized access, or related technical intelligence threats. NSA develops, establishes, and administers comprehensive programs for information security, classification management, security education and motivation, and industrial and personnel security.

## **A-5. Center for Information Systems Security**

The Center for Information Systems Security (CISS) is subordinate to the Defense Information Systems Agency (DISA). The CISS mission is to manage the acquisition, implementation, and integration of INFOSEC products and services into DISA programs and other DOD systems and activities. It also coordinates INFOSEC planning and policy actions throughout DISA. Its goal is to create and manage a unified, fully integrated information systems security program for all defense information infrastructure (DII) systems. CISS acts as the focal point for assuring availability, integrity and confidentiality of DII automated information systems. It develops, coordinates and supports a DOD-wide INFOSEC education, training and awareness program; coordinates the development of the curriculum to support an INFOSEC career field/professional program; and coordinates and executes DOD-wide procedures to identify and disseminate INFOSEC products to meet DOD-wide INFOSEC requirements.

## **A-6. Joint Information Operations Center**

The JIOC was formed from the nucleus of the former Joint Electronic Warfare Center, transitioning from purely EW to encompass all elements of C2W. Under the operational control of the JCS, the JIOC supports the integration of OPSEC, PSYOP, military deception, EW, and destruction throughout the planning and execution phases of an operation. The JIOC provides direct IO tactical and technical analytical support to operational commanders through teams of command and control warfare specialists. Each JIOC team has a habitual relationship with a supported theater. Support is also provided to Secretary of Defense, the Joint Staff, the Services and other government agencies. The JIOC maintains specialized expertise in C2W systems engineering, operational applications, capabilities and vulnerabilities. The JIOC is comprised of a balanced mixture of personnel from all four military services, the civil service and three allied nations. The JIOC and the Air Force Information Warfare Center (AFIWC) are co-located with the Air Intelligence Agency headquarters at Kelly Air Force Base in San Antonio, Texas.

## **A-7. Joint Communications Security Monitor Activity**

The Joint Communications Security (COMSEC) Monitor Activity (JCMA) is an agency of the Joint Chiefs of Staff having IW applications. It was created in 1993 by a Memorandum of Agreement between the Service operations deputies, the Director, Joint Staff, and NSA. It is charged with conducting COMSEC monitoring (collection, analysis, and reporting) of DOD telecommunications and automated information systems and monitoring of related noncommunications signals. It identifies vulnerabilities exploitable by potential enemies and recommends countermeasures and corrective actions. The JCMA focuses on unencrypted DOD systems and does not perform traditional telephone monitoring, which remains a Service responsibility. The Joint Staff J-3 has primary responsibility for JCMA affairs. This facilitates coordination between the JIOC and the JCMA. The JCMA supports both real-world operations, as well as joint exercises and DOD systems monitoring through the following:

- INFOSEC monitoring and analysis support.
- Joint COMSEC monitoring and analysis teams to provide direct, deployable joint COMSEC monitoring support. If tasked, the JCMA may manage all INFOSEC monitoring.
- Cryptographic or plain language system monitoring.
- Timely, tailored reporting to supported commanders, to include near real time reporting of inadvertent disclosure of friendly critical information identified in the OPSEC process.

## **A-8. Joint Spectrum Center**

The Joint Spectrum Center (JSC) was activated in September 1994 under the direction of the Joint Staff's J-6. The JSC assumed all the mission and responsibilities previously performed by the Electromagnetic Compatibility Center, as well as additional functions. It deploys teams in support of the JFCs and serves as the DOD focal point for supporting spectrum supremacy aspects of IW. The JSC assists JFCs in developing and managing the JRFL and assisting in the resolution of operational interference and jamming incidents. While informal coordination occurs on IW related issues between the JSC, the JCMA, and the Joint C2W Center, each organization interfaces separately with the JFC staffs.

The JSC provides support in spectrum planning, electromagnetic compatibility/vulnerability, electromagnetic environmental effects, information systems, modeling and simulation, operations support, and system acquisition to the JFCs, Services, and other government organizations. It also provides—

- Location and technical characteristics of friendly force C2 systems.
- Assistance in developing the JFC's JRFL for deconfliction purposes. The JSC may deploy an augmentation team trained to prepare JRFLs or provide training and assistance in how to prepare a JRFL.
- Assistance in the resolution of operational interference and jamming incidents. The JSC may deploy teams capable of quickly locating and identifying interference sources and recommending technical and operational fixes to resolve identified interference sources.
- Data about foreign command, control, communications, and computers (C4) frequency and location data.
- Unclassified C4 area studies about the regional C4 infrastructure (physical and cultural characteristics, overview of telecommunications systems, and electromagnetic frequencies registered for use within the geographic boundaries of each country in the region.

## **A-9. Joint Warfare Analysis Center**

The JWAC assists the Chairman of the Joint Chiefs of Staff and the combatant commanders in their preparation and analysis of joint operation plans and the Service chiefs' analysis of weapon effectiveness. The JWAC provides analysis of engineering and scientific data and integrates operational analysis with intelligence. The JWAC will normally support a JTF through the supported combatant commander.

## **A-10. Land Information Warfare Agency**

Officially activated in May 1995, LIWA is subordinate to the Army Intelligence and Security Command but is under the operational control of the Headquarters, Department of the Army, Deputy Chief of Staff for Operations. The mission of LIWA is to provide IW/IO support to the land component and major/separate Army commands, active and reserve

component, and to facilitate planning and execution of IO. It draws upon existing capabilities in the Army including PSYOP, EW, and operational security. LIWA provides operational support at the Army corps and higher levels. It will support a MAGTF if it is performing in the capacity of the land component commander.

LIWA often forms task organized IO teams which deploy to support Army commands. LIWA's structure contains a small intelligence organization designed to be the focal point for IO intelligence support. LIWA intelligence analysts provide the deployed teams with sharply focused IO area studies, IO targeting products, and quick-response one-of-a-kind reports. LIWA conducts and participates in studies, war games and exercises designed to identify future IO requirements and capabilities. Models and simulations are developed to support analysis and decisionmaking.

LIWA teams, along with the other JTF components or organizations, support the Army commander's goal of achieving information dominance. LIWA's purpose is to provide Army commands with technical expertise that is not resident on the command's general or special staff, and to exercise technical interfaces with other commands, Service components, and national, DOD, and joint information centers. When deployed, LIWA field support teams become an integral part of the command's IO staff. To facilitate planning and execution of IO, LIWA provides IO/C2W operational support to land component and separate Army commands, and reserve components commands as required.

## **A-11. Naval Information Warfare Activity**

The Navy established the Navy Information Warfare Activity (NIWA) in August 1994 to serve as their focal point for IW activities. Directly subordinate to the Naval Security Group, NIWA is located at Fort Meade, Maryland and is closely linked to the NSA. NIWA is the Navy's principal technical agent to research, assess, develop, and prototype IW capabilities in all aspects of IW attack, protect and exploit. It acquires and analyzes state-of-the-art technologies (software and hardware), evaluates fleet applicability and prototype developmental capabilities. NIWA has developed the IW Mission Planning, Analysis, and Command and Control

Targeting System tool for tactical commanders. NIWA is the Navy's interface with other Service and national IW organizations, working closely with the FIWC to develop of IW technical capabilities for Navy and joint operations.

## **A-12. Fleet Information Warfare Center**

The Navy established the FIWC at Little Creek, Virginia from existing Fleet Deception/C2W Group assets. The FIWC serves as the link between the NIWA and the Atlantic and Pacific Fleets. With personnel deployed on carrier battle groups throughout the world, the FIWC fulfills a similar mission for the Navy that the JIOC does for the JFC. The IW organizational structure created by the Navy enables the FIWC to focus on near-term operational requirements, while the NIWA assumes a more long-term perspective keeping abreast of IW advances and developing and acquiring systems.

## **A-13. Air Force Information Warfare Center**

The AFIWC was originally activated as the 6901st Special Communications Center on 1 July 1953. In July 1975, it was redesignated as the Air Force Electronic Warfare Center. Its successes against Iraqi C2 systems in Operation Desert Storm led to the realization that the strategies and tactics of C2W could be expanded to the entire information spectrum and be implemented as IW. The AFIWC was activated in September 1993 with elements from the former center and Air Force Cryptologic Support Center's Securities Directorate. It is collocated with both the Air Intelligence Agency and the JIOC at Kelly Air Force Base, Texas. Personnel from the AFIWC regularly team with the JOIC on major deployments. The AFIWC serves as the Air Force C2W executive agent with approximately 1000 military and civilian personnel assigned. The AFIWC explores, applies, and migrates offensive and defensive information warfare capabilities for operations, acquisition and testing.

AFIWC conducts integrated C2W analysis studies on designated adversaries. Such studies, collectively are termed SENSOR HARVEST. Information used in SENSOR HARVEST is derived from all-source intelligence, databases, and models. AFIWC also produces and maintains

the Functional Networks (CONSTANT WEB) within the DOD's Military Integrated Data Base providing U.S. combat forces with crucial enemy C2 network information. It contains multi-source intelligence, depicting a comprehensive picture of the military command, control, and communications (C3), identifying critical nodes for selected countries.

## **A-14. 4<sup>th</sup> Psychological Operations Group**

The 4th Psychological Operations Group (Airborne) at Fort Bragg, N.C., the only active Army psychological operations unit, and constitutes 26 percent of all U.S. Army psychological operations units. The remaining 74 percent are in the reserve component.

Tactical psychological operations are used to secure immediate and near-term goals. These PSYOP activities serve as a means to lower the morale and efficiency of enemy forces. Both tactical and theater-level psychological operations may be used to enhance peacetime military activities of conventional and special operations forces operating in foreign countries. Cultural awareness packages attune U.S. forces before deploying overseas. In theater, media programs publicize the positive aspects of combined military exercises and deployments.

## **A-15. 96<sup>th</sup> Civil Affairs Command**

The 96th Civil Affairs Command, with four percent of the CA forces, is the only active Army CA unit. The unit is readily available to deploy and provides primarily tactical support. The remaining 96 percent of the Army's CA forces are found in the reserve component. The command identifies critical requirements needed by local citizens in war or disaster situations. It can also locate civil resources to support military operations, help minimize civilian interference with operations, support national assistance activities, plan and execute non-combatant evacuation, support counter-drug operations, and establish and maintain liaison or dialogue with civilian personnel agencies and civilian commercial and private organizations. CA may provide functional expertise for foreign internal defense operations, unconventional warfare operations and direct action missions. It may also conduct emergency coordination and administration where civilian political-economic structures have been incapacitated.

## **A-16. 193<sup>rd</sup> Special Operations Wing**

The 193rd Special Operations Wing provides an airborne electronic broadcasting system installed on five EC- 130E (RR) COMMANDO SOLO aircraft. This is the only U.S. Air Force asset whose mission is to support PSYOP by broadcasting programs in the standard AM/FM radio, television, short wave, and military communication bands. The 193rd performs this unique mission with six specially configured EC130E/RR aircraft. This system may also be used in a CA and/or public information role, to support disaster assistance efforts by broadcasting public information and instructions for evacuation procedures, and to temporarily replace damaged transmitters during evacuation operations.

A secondary mission assigned to the 193d is providing electronic counter measures in the military frequency spectrum for the Air Force Intelligence Command, SENIOR SCOUT mission. This mission is performed with two specially modified EC130E aircraft.

---

## Appendix B

# MAGTF Information Operations Assets

---

## B-1. 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.

## B-2. 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.

### **B-3. 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.

### **B-4. 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. This support can include the use of shore-based loudspeaker broadcasting, aerial and artillery leaflet dissemination, combat camera documentation, and use of motion picture projection and viewing equipment.

### **B-5. 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.

This page intentionally left blank.

---

## Appendix C

# Operation Order Formats

---

Writing of the operations order is conducted during the final (orders development) phase of planning, and is essential to ensuring the integration of all the IO disciplines, to include OPSEC, military deception, PSYOP, EW, physical destruction and other capabilities. The process begins in the basic order with the provision of sufficient guidance in the commander's intent and concept of operations to conduct detailed IO planning and execution.

This annex provides the format for the remaining sections of an operations order in which IO instructions should be contained. Appendix 6 to Annex B, Intelligence, addresses specific IO intelligence requirements. Appendix 3 to Annex C, Operations, is the basic IO/C2W document that clearly states the primary missions of each of the elements of IO/C2W. It provides the necessary guidance to ensure that the elements are all working toward the accomplishment of the IO/C2W mission. Detailed execution instructions for each of the five major IO/C2W elements (military deception, EW, OPSEC, PSYOP, and physical destruction) should be included in the tabs to the IO/C2W appendix. A separate appendix addresses force protection aspects of IO.

Annex S contains guidance for special technical operations, and Annex U will provide information regarding defensive IO against CNA and information assurance.

CLASSIFICATION

## C-1. Intelligence Support to C2W Appendix Format

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

APPENDIX 6 TO ANNEX B TO (Number) (Operation CODEWORD) ()  
INTELLIGENCE SUPPORT TO COMMAND AND CONTROL  
WARFARE ()

( ) REFERENCES. List references pertinent to the plan.

### 1. ( ) General

a. ( ) Purpose. This appendix will focus on the who, what, where, when, why, and how of employing intelligence assets in support of C2W as detailed in Annex C. Annex B, Appendix 2, and Annex C, Appendix 3, of this publication should be referenced for details on SIGINT support to C2W.

b. ( ) Relationships. Specify command or theater-unique relationships between intelligence, C2W, and user organizations. Explain specific functions, responsibilities, and data flow; and the relationships between OPSEC, PSYOP, and military deception planners and the intelligence staff.

### 2. ( ) Mission, Threat, and Requirements

a. ( ) Mission. Define the mission for intelligence support to C2W.

b. ( ) Threat Estimates. Include and refer to estimates of enemy electromagnetic capabilities in Annex B. Evaluate types of threats to friendly weapon platforms and systems, critical C4 for weapons

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

control, target acquisition, and surveillance systems. Describe the politico-military situation and strategies; provide leadership profiles and describe influential group attitudes; describe enemy organizational structure, military intentions, and doctrine; outline the organization and capabilities of enemy intelligence systems; and describe enemy C2 systems.

c. ( ) Operational Requirements. Address specific user requirements that drive intelligence support to C2W. In addition, include general narrative statements of functional user requirements (e.g., flagging of foreign radar operating parameters in support of EW reprogramming).

d. ( ) Information Requirements. List information requirements (IRs) required to support C2W or refer to the coordinating instructions of the basic operation order or plan, the priority information requirements section of Annex B, or Appendix 1 to Annex B. Specify procedures to ensure timely fulfillment of EW IR, including real-time dissemination in the tactical situation. Also specify procedures to provide immediate feedback and evaluations on enemy reactions to deception actions and PSYOP messages, and acquisition of OPSEC indicators.

3. ( ) Collection. See Annex B.

a. ( ) Collection Management. Address how the collection managers will support planners, analysts, and targeteers in their support of C2W. Include definition and prioritization of requirements after coordination with the operations staff.

b. ( ) Supporting Systems. Address how collection assets support the acquisition of data used to support C2W and specify required imagery intelligence (IMINT), including how to obtain it and other required operational data. Establish procedures for OPSEC and military deception planners to assist intelligence systems personnel to penetrate enemy OPSEC measures and military deceptions.

c. ( ) Capabilities Analysis. Address required versus current capabilities and capacities for collection to support this plan and identify shortfalls.

(Page Number)

CLASSIFICATION

## CLASSIFICATION

Consider not only technical capabilities, but also actual capacities of current collectors in relation to the projected volume of IRs.

### 4. ( ) Processing, Production, Application, and Dissemination

a. ( ) Communication With Collection Management. Explain how data receivers, correlators, and analysts will communicate with collection management people.

b. ( ) Coordination. Explain how OPSEC, PSYOP, and military deception planners will communicate with intelligence planners.

c. ( ) Correlation. Address where intelligence support of C2W fits in with existing correlation programs, how the data is provided to the operator, and coordination for frequency deconfliction.

d. ( ) Foreign Capability or Activity Assessment. Address specific reporting, C2W tactics and techniques studies, order of battle, and other products on the enemy that would provide intelligence to C2W. Include identification and vulnerability assessments of enemy-critical electromagnetic links, nodes, sensors, and weapon systems. Identify shortfalls in intelligence support.

e. ( ) Targeting. Explain the relationship between the target analyst and analysts performing foreign capability or activity assessment, data base management, and operations. Include targeting support to C2W in Annex B and Appendix 4 to Annex B.

f. ( ) Data Base Management. Define applicable data bases and address command participation in data bases supporting C2W. Evaluate adequacy, accuracy, and timeliness of the data to support the plan and discuss plans for updating and integrating applicable data bases.

g. ( ) EW Reprogramming. Specify details of supporting reprogramming.

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

h. ( ) C3 Network Analysis. Specify who will perform C3 network analysis.

i. ( ) Capabilities Analysis. Address required versus existing capabilities and capacities in production, processing, and application of intelligence to support C2W in this plan.

### 5. ( ) Sustaining Functions

a. ( ) Automated Data Processing. Address both hardware and software needed to provide intelligence support to C2W.

b. ( ) Communications. Address communications systems unique to intelligence support to C2W. If applicable, reference Annexes B and K and any other key documents that describe intelligence system communications.

c. ( ) Capabilities Analysis. Address required versus existing capabilities to provide intelligence ADP and communications support to C2W.

## ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

OFFICIAL:

s/

Name

Rank and Service

Title

(Page Number)  
CLASSIFICATION

CLASSIFICATION

**C-2. Information Operations/C2W Appendix Format**

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

APPENDIX 3 TO ANNEX C TO OPERATION ORDER OR PLAN  
(Number) (Operation CODEWORD) ( )  
INFORMATION OPERATIONS/COMMAND AND CONTROL  
WARFARE ( )

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

1. ( ) Situation. Summarize the overall operational situation as it relates to IO/C2W.

a. ( ) Enemy. Summarize the enemy situation, force disposition, intelligence capabilities, and possible courses of action. If applicable, reference intelligence estimates or summaries. Address any specific information that bears directly on the planned IO/C2W operation.

b. ( ) Friendly. Summarize the situation of those friendly forces that may directly affect attainment of IO/C2W objectives. Address any critical limitations and any other planned IO/C2W operations.

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

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

2. ( ) Mission. State the IO/C2W mission in a clear, concise statement that answers the questions: Who, what, when, where, and why.

3. ( ) Execution

a. ( ) Concept of Operations. Summarize how the commander visualizes the execution of IO/C2W from its beginning to its termination. Describe how the IO/C2W operation will support the command's operational mission. Summarize the concepts for supervision and termination of IO/C2W operations.

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

(2) ( ) When an operation involve various phases (i.e., peace or pre-hostilities, crisis, war, post-hostilities etc.), the concept of operations should be prepared in subparagraphs describing the role of IO/C2W in each phase.

(3) ( ) The concepts for offensive and defensive IO/C2W may be addressed in separate subparagraphs.

b. ( ) Information Operations/Command and Control Warfare Tasks. Identify the major tasks for each of the five elements of IO/C2W. Note: The five elements of IO/C2W listed below are covered in tabs A through E.

(1) ( ) Military deception.

(2) ( ) Electronic warfare.

(3) ( ) Operations security.

(4) ( ) Psychological operations.

(5) ( ) Physical destruction.

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

- c. ( ) Coordinating Instructions. Address any mutual support issues relating to the elements of IO/C2W.
4. ( ) Administration and Logistics. Address any IO/C2W-related administrative or logistic requirements.
5. ( ) Command and Control. List any IO/C2W-related C2 instructions. State the command structure for IO/C2W operations. Identify any special IO/C2W communications and reporting requirements.

## ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

## TABS:

- A — Military Deception
- B — Electronic Warfare
- C — Operations Security
- D — Psychological Operations
- E — Physical Destruction

## OFFICIAL:

s/  
Name  
Rank and Service  
Title

(Page Number)  
CLASSIFICATION

CLASSIFICATION

**C-3. Military Deception Tab Format**

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

TAB A TO APPENDIX 3 TO ANNEX C TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ( )  
MILITARY DECEPTION ( )

( ) REFERENCES: Identify plans, documents, maps, and charts that are essential to the effective execution of military deception.

1. ( ) Situation

a. ( ) General. See basic operation order or plan.

b. ( ) Enemy

(1) ( ) General Capabilities. Identify enemy military capabilities directly relating to the planned deception.

(2) ( ) Deception Targets. Describe the political, military, or economic decisionmakers (or organizations) targeted by the deception plan. Include personalities, strengths, weaknesses, vulnerabilities and people or factors known to influence decisions.

(3) ( ) Target Biases and Predispositions. Provide information on known biases and predispositions of political, military, or economic decisionmakers (or organizations).

(4) ( ) Probable Enemy Course of Action. Refer to Annex B (Intelligence).

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

c. ( ) Friendly. Summarize the friendly situation, critical limitation, and concept of operations.

d. ( ) Assumptions. List all assumptions on which the deception is based.

### 2. ( ) Mission

a. ( ) Operational Mission. Extract from paragraph 2 of the basic operation order or plan.

#### b. ( ) Deception Mission

(1) ( ) Deception Goal. Describe the desired effect or the end state a commander wishes to achieve (commander's concept for the deception operation). For example, "To cause the enemy to weight his defense in the eastern corridor; To mislead the enemy as to the time and place of forcible entry operations; To cause dissension within the enemy coalition such that ...."

(2) ( ) Deception Objective(s). List the desired action or inaction by the enemy at the critical time and location.

(3) ( ) Desired Enemy Perceptions. Describe what the deception target must believe for it to make the decision that will achieve the deception objective.

(4) ( ) Deception Story. Outline a scenario of friendly actions or capabilities that will be portrayed to cause the deception target to adopt the desired perception. This could be an alternate COA to the one chosen for the order or plan itself.

### 3. ( ) Execution

#### a. ( ) Concept of the Operation

(1) ( ) General. Generally describe the framework for the operation. Include a brief description of the phases of the deception operation.

(Page Number)

CLASSIFICATION

## CLASSIFICATION

- (2) ( ) Other Information Operations/Command and Control Warfare Elements. Discuss the use of other IO/C2W elements in support of the deception operation. Discuss all other IO/C2W element plans and operations pertinent to the deception. Include coordination required to deconflict if necessary.
- (3) ( ) Feedback and Monitoring. Provide a general statement of the type of feedback expected, if any, and how it will be collected (monitored). Include a brief statement on the impact of the absence of feedback on the plan.
- (4) ( ) Means. Describe available deception assets.
- (5) ( ) Tasks. Specify execution and feedback taskings to organizations participating in the execution and monitoring of the deception operation.
- (6) ( ) Risks. Give a brief risk analysis in the categories given below. Rate risk as low, moderate or high in each category. Refer to Exhibit 3 (Operations) to this tab for detailed risk analyses.
- (a) ( ) Deception is successful. Include likely enemy response. Describe impact on friendly forces from enemy intelligence sharing.
  - (b) ( ) Deception fails. Describe the impact if the target ignores the deception or fails in some way to take the actions intended.
  - (c) ( ) Deception is compromised to allies or adversaries.
- b. ( ) Coordinating Instructions. Identify any tasks or instructions pertaining to two or more of the units listed in the preceding subparagraphs. List the tentative D-day and H-hour, if applicable, and any other information required to ensure coordinated action between two or more elements of the command.

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

4. ( ) Administration and Logistics. State instructions regarding administrative and logistics support procedures to be used in developing, coordinating, and implementing the deception plan. Do not include those administrative, logistic, and medical actions or ploys that are an actual part of the deception operation. Place detailed instructions in Exhibit 4 (Administration and Logistics).

a. ( ) Administration

(1) ( ) General. Outline general procedures to be employed during planning, coordination and implementation of deception activities.

(2) ( ) Specific. Detail any special administrative measures needed to execute the deception operation.

b. ( ) Logistics. Detail logistics requirements for the execution of the deception operation, such as the transportation of special material, or provision of printing equipment and materials. Do not include executions conducted by logistics elements as part of the portrayal of observables. Place detailed instructions in Exhibit 4 (Administration and Logistics).

c. ( ) Costs. As applicable.

5. ( ) Command, Control and Communications

a. ( ) Command Relationships. Use Exhibit 5 (Command Relationships) to illustrate command relationships by phase if required.

(1) ( ) Approval. State approval authority for execution and termination.

(2) ( ) Authority. Designate supported and supporting commanders, supporting agencies as applicable, and any caveats to Exhibit 1 (Task Organization) or Exhibit 5 (Command Relationships).

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

(3) ( ) Oversight. Detail oversight responsibilities particularly for executions by nonorganic units or organizations outside the chain of command.

(4) ( ) Coordination. Identify coordination responsibilities and requirements related to deception executions and execution feedback. Address in-theater and out-of-theater requirements.

b. ( ) Communications. Detail communications means and procedures to be used by control personnel and participants in the deception operation. Include all reporting requirements.

### 6. ( ) Security

a. ( ) General. Outline general procedures to be employed during planning, coordination, and implementation of deception activities.

b. ( ) Specific. State access restrictions, handling instructions, and who has authority to grant access to the deception appendix or plan. Describe use of cover stories if applicable, codewords, nicknames, and procedures for planning and execution documents. If required, place access rosters and other detailed security considerations in a separate document.

## ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

## EXHIBITS:

- 1 — Task Organization
- 2 — Intelligence
- 3 — Operations
- 4 — Administration and Logistics

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

- 5 — Command Relationships
- 6 — Execution Schedule
- 7 — Distribution

OFFICIAL:

s/

Name

Rank and Service

Title

(Page Number)  
CLASSIFICATION

CLASSIFICATION

**C-4. Electronic Warfare Tab Format**

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

TAB B TO APPENDIX 3 TO ANNEX C TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ( )  
ELECTRONIC WARFARE ( )

( ) REFERENCES: Identify plans, documents, maps, and charts that are essential to the effective execution of electronic warfare.

1. ( ) Situation

a. ( ) Enemy Forces. Provide an estimate of the capabilities, limitations, and vulnerabilities of enemy communications, non-emitting, and EW systems, including the ability to interfere with the accomplishment of the EW mission. If applicable, refer to Annex B and the current intelligence estimate.

b. ( ) Friendly Forces. Provide a summary of friendly EW facilities, resources, and organizations that may affect EW planning by subordinate commanders. Include friendly foreign forces with which subordinate commanders may operate.

c. ( ) Assumptions. State any assumptions about friendly or enemy capabilities and courses of action that significantly influence the planning of EW operations.

2. ( ) Mission. Provide a clear and concise statement of the EW mission (who, what, when, why, and where).

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

### 3. ( ) Execution

#### a. ( ) Concept of Operations

(1) ( ) Describe the role of EW in the commander's IW strategy. Summarize the scope of EW operations and the methods and resources to be employed, including the employment of organic and nonorganic capabilities. Address how EW will support the other elements of IW.

(2) ( ) The concept of operations may be a single paragraph or divided into two or more subparagraphs depending upon the complexity of the operation.

(3) ( ) In phased operations, the concept of operations may have separate subparagraphs for each phase.

b. ( ) Tasks. In separate numbered subparagraphs, assign individual EW tasks and responsibilities to each component or subdivision of the force. Include all instructions that are unique to that component or subdivision.

#### c. ( ) Coordinating Instructions

(1) ( ) List any instructions applicable to two or more subdivisions or components.

(2) ( ) Identify any requirements for the coordination of EW actions between subordinate elements.

(3) ( ) Provide guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered elsewhere in the tab.

(4) ( ) Provide EMCON guidance. Address detailed or lengthy guidance in an exhibit to this tab.

(5) ( ) Coordinate with G-6 to create the JRFL.

(Page Number)

CLASSIFICATION

CLASSIFICATION

4. ( ) Administration and Logistics

a. ( ) Administration. Include necessary administrative guidance. Provide examples of any required reports.

b. ( ) Logistics. Provide special instructions on logistics support for EW operations.

5. ( ) Command and Control

a. ( ) Feedback. Describe the concept for monitoring the effectiveness of EW operations during execution. Identify specific intelligence requirements for feedback.

b. ( ) After-Action Reports. Identify any requirements for after-action reporting.

c. ( ) Signal. Address any special or unusual EW related communications requirements.

ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

OFFICIAL:

s/

Name

Rank and Service

Title

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

### C-5. Operations Security Tab Format

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

TAB C TO APPENDIX 3 TO ANNEX C TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ( ) OPERATIONS SECURITY ( )

( ) REFERENCES: Identify plans, documents, maps, and charts that are essential to the effective execution of operations security.

#### 1. ( ) Situation

##### a. ( ) Enemy Forces

(1) ( ) Current Enemy Intelligence Assessment. State the estimated enemy's assessment of friendly operations, capabilities, and intentions. Specifically address any known enemy knowledge of the friendly operation addressed in the basic plan.

(2) ( ) Enemy Intelligence Capabilities. State the enemy's intelligence collection capabilities by major categories (SIGINT, HUMINT, IMINT, etc.). Address all potential sources to include the capabilities of any nations that may provide support to the enemy. Describe how the enemy's intelligence system works to include the time needed for intelligence to reach key decisionmakers. Identify major analytical organizations and key personalities. Discuss unofficial intelligence organizations, if any, that support the national leadership. Identify strengths and weaknesses.

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

### b. ( ) Friendly Forces

(1) ( ) Friendly Operations. Briefly describe the major actions to be conducted by friendly forces in the execution of the basic plan.

(2) ( ) Critical Information. List the identified critical information. Include the critical information of higher headquarters. In phased operations, list the critical information by phase because information that might be critical in one phase may not require protection in later phases.

c. ( ) Assumptions. Identify any assumptions upon which this OPSEC plan is based.

2. ( ) Mission. Provide a clear and concise statement of the OPSEC mission (who, what, when, why, and where).

### 3. ( ) Execution

a. ( ) Concept of Operations. Discuss the role of OPSEC in the commander's IW strategy. Describe the general concept for implementing planned OPSEC measures. Describe by phase and major activity (maneuver, logistics, communications, etc.), if appropriate. Address OPSEC support to other elements of IW.

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

(2) ( ) In phased operations, the concept of operations may have separate subparagraphs for each phase.

b. ( ) Tasks. Identify specific OPSEC measures to be executed. List by phase, if appropriate. Assign responsibility for execution to appropriate subordinate elements. Particularly detailed or lengthy listings should be added as an exhibit to this tab.

c. ( ) Coordinating Instructions. Identify any requirements for coordinating OPSEC measures between subordinate elements. Address

(Page Number)

CLASSIFICATION

## CLASSIFICATION

required coordination with PA. Provide guidance on terminating OPSEC related activities. Address the declassification and public release of OPSEC-related information.

4. ( ) Administration and Logistics. Address any special OPSEC-related administrative or logistic support requirements. List any administrative or logistics related OPSEC measures in subparagraph 3.

5. ( ) Command and Control

a. ( ) Feedback. Describe the concept for monitoring the effectiveness of OPSEC measures during execution. Identify specific intelligence requirements for feedback.

b. ( ) OPSEC Surveys. Address any plans for conducting OPSEC surveys in support of this operation.

c. ( ) After-Action Reports. Identify any requirements for after-action reporting.

d. ( ) Signal. Address any special or unusual OPSEC related communications requirements. List all communications related OPSEC measures in subparagraph 3.

## ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

OFFICIAL:

s/  
Name  
Rank and Service  
Title

(Page Number)  
CLASSIFICATION

CLASSIFICATION

## C-6. Psychological Operations Tab Format

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

TAB D TO APPENDIX 3 TO ANNEX C TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ( )  
PSYCHOLOGICAL OPERATIONS ( )

( ) REFERENCES: List plans, estimates, basic PSYOP studies, special PSYOP studies, special PSYOP assessments, and other documents that have a significant bearing on the conduct of PSYOP.

1. ( ) Situation. Summary of the psychological situation in the area of operations, any on-going PSYOP programs and any significant factors influencing PSYOP activities. (If parts of the situation description are long or complex, include as attachments.)

a. ( ) Overview. Describe the general situation, competing goals, and the task to be accomplished.

b. ( ) US (or US and Allied) Perspective. Briefly outline intentions (how the assigned task will be accomplished), capabilities (resources to be used), and activities (current actions and general phasing of future actions).

c. ( ) Neutral Perspective (if applicable). Briefly outline estimated neutral intentions under various circumstances, the resources available to them, and their activities. State neutral actions and behavior that would favor mission accomplishment. Indicate apparent current COAs that might affect mission accomplishment and summarize resources available to execute alternative COAs. (Include the abilities to execute

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

IW strategies.) State objective and subjective factors that could affect decisions and resource effectiveness. Identify staff factions and particularly influential individuals. Describe the characteristics of decisionmakers, their key advisers; major staff planners; staff factions, particularly influential individuals; and intelligence system analysts. List groups of related planner and decisionmaker EEFI. For each group list estimates of background knowledge and desired and harmful appreciations.

### d. ( ) Enemy Perspectives

(1) ( ) Decisionmaker and Staff. Identify the decisionmakers who can direct development or allocation of resources of COA execution pertinent to the task assigned. Outline feasible, alternative actions that would favor or harm friendly operational effectiveness. Indicate COAs that might affect friendly task accomplishment and summarize resources available to execute each COA. Describe the characteristics of enemy decisionmakers, their key advisors and staff (particularly intelligence analysts).

(2) ( ) Intelligence Systems. Identify intelligence systems that support decisionmakers and their staffs. Summarize intelligence systems' capabilities pertinent to the situation. Cite references for detail. Describe objective and subjective factors and the characteristics of collection planners and decisionmakers that affect their development and selection for use of information gathering resources. List groups of related collection planner and decisionmaker EEFI and for each group list, estimates of background knowledge and desired and harmful appreciations.

(3) ( ) Target Audiences. Identify groups that can influence plans, decisions, and operational effectiveness in task accomplishment; identify their susceptibility to PSYOP. State group behavior favorable and harmful to task accomplishment. Briefly describe the apparent goals, motivations, and characteristics of each group and the leaders who can cause groups to behave in various ways. List

(Page Number)

CLASSIFICATION

## CLASSIFICATION

groups of related target audience EEFI and, for each group, list estimates of background knowledge as well as desired and harmful appreciations.

(4) ( ) Command Systems. Describe communication systems and command centers used to plan COAs and control, coordinate, and supervise execution of the planned COA. Briefly identify the purpose of each command and control communications net and its characteristics. State targets for jamming or attacking. Indicate when to execute operations to demoralize and disorganize opposing command, reduce opposing operational effectiveness, enhance the effectiveness of planned deceptions and PSYOP, and support OPSEC to the maximum advantage.

2. ( ) Mission. State how the PSYOP mission will support the maneuver commander. Conduct PSYOP to persuade the following target audiences to adopt the attitudes and to behave as indicated.

3. ( ) Execution

a. ( ) Concept of Operations

(1) ( ) Overview. State the commander's intent. Outline the overall concept for using PSYOP in support of task accomplishment. Sequentially address strategic PSYOP in peacetime and in support of preconflict deterrence options; strategic and theater PSYOP in support of sustained hostilities (conduct of war globally or in a region, and support for campaigns and operations); and joint tactical PSYOP in support of operational COAs. State who will plan and conduct each PSYOP and the supporting commanders.

(2) ( ) Provide the following as general guidance to units and forces involved:

(a) ( ) Valid PSYOP themes to be promoted to induce strategic and theater PSYOP objectives.

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

(b) ( ) Valid or invalid PSYOP themes to be discouraged and indications of specific target audience sensitivities and harm that might occur if the themes are accepted by target audiences.

(c) ( ) PSYOP actions suitable for use:

1. ( ) Guidance for the conduct of military operations and actions, and personnel behavior, to promote valid PSYOP themes.

2. ( ) Guidance for avoiding military operations and actions, and personnel behavior, that would result in harmful target audience attitudes and behavior.

3. ( ) Description of the cultural and psychological characteristics of target audiences to aid operational planners and personnel in selecting COAs and interacting with target audience members.

(d) ( ) Description of enemy PSYOP (including disinformation) directed at U.S. personnel and at foreign groups in the operational area and guidance for countering such enemy operations.

(3) ( ) Provide an outline of each planned PSYOP operation. Indicate for each target audience and set of PSYOP objectives, overall themes, subgroups to be targeted, their characteristics, and specific themes to be promoted for each subgroup. As appropriate, refer to intelligence and PSYOP studies. State provisions for testing, producing, stocking, and disseminating PSYOP materials and for measuring PSYOP effectiveness. Describe command and staff arrangements for each campaign or operation and indicate supporting commanders. List resources required to plan and conduct PSYOP actions, including civil capabilities, indigenous assets, exploitation of enemy prisoners of war (EPWs), internees, and detainees for PSYOP, and military PSYOP resources. State logistic requirements, including preparation, distribution, and

(Page Number)

CLASSIFICATION

## CLASSIFICATION

stocking of PSYOP materials; transport of PSYOP material and personnel to operational areas and their basing and support while conducting PSYOP; provisions for the supply and maintenance of U.S. and indigenous PSYOP material; and fiscal and personnel matters. Indicate requirements for implementing schedules and PSYOP operation control sheets. (Note: Handle plans for PSYOP conducted in support of UW operations, by SO forces in support of military deceptions as OPSEC-sensitive. Assign each plan a codeword and distribute it separately from the basic operation order or plan and PSYOP appendix.)

(4) ( ) In the basic concept description and in each tab describing separate operations, provide OPSEC planning guidance. The guidance should address planning for, preparing for, and conducting PSYOP and PSYOP actions to maintain essential secrecy for the commander's intentions and to gain and maintain essential secrecy for OPSEC-sensitive PSYOP COAs.

b. ( ) Situation Monitoring. Describe how intelligence, multidiscipline CI, security monitoring, and operational feedback will be provided. State requirement for running situation estimates; periodic estimates of target appreciations responsive to EEFI, actions, and attitudes and behavior; and current reporting of intelligence and multidiscipline CI information, security monitoring results, and implementing actions. Identify resources required and their availability.

c. ( ) Control. Outline how control will be affected and implementation centrally coordinated. State coordinating instructions. Describe accomplishment of implementation planning and supervision of the planned action. Identify the need for specific PSYOP operations. Address coordination with adjacent commands and civilian agencies, including U.S. diplomatic missions, USIA, and the Agency for International Development. Also address coordination with military deception, OPSEC, and EW planners, and planners in the fields of civic action, humanitarian assistance, CA, EPW, CI, C3, legal, captured U.S. personnel, and operations.

(Page Number)

CLASSIFICATION

## CLASSIFICATION

d. ( ) Tasks. Assign responsibilities to implement the concept. When multiple organizations are involved, designate an executive agent to coordinate implementation. Ensure that tasks clearly fix responsibilities and provide for feedback about effectiveness.

4. ( ) Administration and Logistics. Provide a statement of the administrative and logistic arrangements applicable to PSYOP but not covered in the basic operation order or plan or another annex. Include data on:

a. ( ) Logistics

(1) Stocking of propaganda and information materials and provisions to disseminating organizations.

(2) ( ) Provisions for the supply and maintenance of PSYOP-unique supplies and equipment.

(3) ( ) Provisions for control and maintenance of indigenous equipment and materials.

(4) ( ) Fiscal matters relating to special funds.

(5) ( ) Personnel matters relating to indigenous personnel.

b. ( ) Administration

(1) ( ) Requirements for special reports.

(2) ( ) Requirements for planning and operations in support of education programs regarding EPWs and civilian internees.

(3) ( ) Participation in interrogation of EPWs, internees, and detainees to obtain information essential for or peculiar to PSYOP.

5. ( ) Command and Control. Refer to appropriate sections of Annex K and provide pertinent extracts of information included in the basic operation order or plan or Annex K, including:

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

- a. ( ) Recognition and identification instructions.
- b. ( ) Electronic policy.
- c. ( ) Headquarters locations and movements.
- d. ( ) Codewords.
- e. ( ) Frequency allocation.

Tabs: If too lengthy for inclusion in the body of this appendix, place any information required above in a tab. In each case, refer to the tab in the appropriate paragraphs of the appendix.

## ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

OFFICIAL:

s/

Name

Rank and Service

Title

(Page Number)  
CLASSIFICATION

CLASSIFICATION

## C-7. Physical Destruction Tab Format

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

TAB E TO APPENDIX 3 TO ANNEX TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ( )  
PHYSICAL DESTRUCTION ( )

( ) REFERENCES: List plans, estimates, studies, and other documents that have a significant bearing on C2 and infrastructure destruction.

1. ( ) Situation. In addition to references to current intelligence at Annex B of the basic operation order or plan, describe the politico-military and military situation expected at the time the plan would be executed and the competing U.S. and foreign objectives.

a. ( ) Enemy Situation. Describe the general situation in the target country.

b. ( ) Friendly Situation. Summarize the situation of those friendly forces (higher, adjacent, supporting, and reinforcing) that may directly affect C2 and key infrastructure destruction operations. Address any critical limitations and any other planned IW operations.

c. ( ) Assumptions. Identify any assumption on which this plan is based.

2. ( ) Mission. Provide a clear and concise statement of C2 and infrastructure physical destruction.

3. ( ) Execution. Summarize how the commander visualizes the execution of this supporting plan to the IW plan from its beginning to its termination.

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

The overview should include a broad definition of the phases of the operation, and the JFC's intent and the desired end state. Complex plans should include a detailed scheme of support categorized by phases.

- a. ( ) Tasks for Subordinate Commands. Identify the major tasks of each subordinate command.
- b. ( ) Coordinating Instructions. Include ROE references that impact the C2 and infrastructure destruction plan.
4. ( ) Administration and Logistics. Provide a statement of applicable administrative and logistic arrangements not covered in the basic operation order or plan.
5. ( ) Command and Control. Provide a statement of applicable command and control arrangements not covered in the basic operation order or plan.

## ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

OFFICIAL:

s/

Name

Rank and Service

Title

(Page Number)  
CLASSIFICATION

CLASSIFICATION

**C-8. Force Protection Appendix Format**

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

APPENDIX 15 TO ANNEX C TO OPERATION ORDER OR PLAN  
(Number) (Operation CODEWORD) ( )  
FORCE PROTECTION ( )

( ) REFERENCES: Cite references necessary for a complete understanding of this appendix. List DOD publications, command directives, service regulations, policy regulations, operational manuals, and locally published directives and regulations that amplify this appendix. Examples include: DOD Dir 5200.8, “Security of Military Installations and Resources”; DOD Dir 2000.12, “Protection of DOD Personnel and Resources Against Terrorist Acts.”

1. ( ) Situation

- a. ( ) Enemy. See Annex B (Intelligence). Define the enemy from a force protection perspective. Outline the threat across all phases of the plan.
- b. ( ) Friendly. See Task Organization. List the forces available to support the protection plan. Highlight police agencies, military and non-military, including HN agencies if applicable. In each tab highlight any special troops available to deal with each applicable aspect of force protection.
- c. ( ) Assumptions. List all assumptions on which this appendix is based.

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

- d. ( ) Resource Availability. List resource availability.
  - e. ( ) Planning Factors. List applicable planning factors.
2. ( ) Mission. State the force protection mission. Since the mission may change as the intensity of the operation changes, more than one subparagraph may be required.
  3. ( ) Execution. Because the force protection activities will change with the commander's emphasis, enemy activities, and the predominant threat during the prosecution of an operation, separate paragraphs for each phase of the operation may enhance the understanding of the plan.
    - a. ( ) Concept of Operations. Generally describe the commander's vision of the operation and describe what will be done to protect the force.
    - b. ( ) Tasks. Assign tasks and responsibilities necessary to complete the mission. This brief description should be followed by details in the appropriate tab to this appendix.
    - c. ( ) Coordinating Instructions. Include instructions applicable to two or more units. Appropriate instructions include HN law enforcement coordination and interplay with other support agencies (e.g., PA).
  4. ( ) Administration and Logistics
    - a. ( ) Logistics. List any special equipment needed for the support of the force protection program. Identify command points of contact and special equipment funding either here or in the tabs.
    - b. ( ) Administration. Describe the measures peculiar to the administration and prosecution of the force protection plan.
    - c. ( ) Reports. Describe the command's requirements for reporting force protection activities. Outline the information to be provided to subordinate units and describe the reports required from subordinate

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

units. Include the means of communication desired (email, letter, radio, etc.).

### 5. ( ) Command and Control

a. ( ) Command Relationships. Refer to Annex J (Command Relationships). Describe in detail any special command relationships. Emphasis must also be given to “appeal authority” needed to resolve differences that may arise in the resolution of some aspect of the force protection operation (e.g., use of force to neutralize a hostage situation).

b. ( ) C3 Systems. Identify C3 system requirements for support of the force protection mission. Refer to Annex K (Combat Information Systems).

## ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

## ENCLOSURES:

- A — Combating Terrorism
- B — Physical Security
- C — Base Defense

## OFFICIAL:

s/

Name

Rank and Service

Title

(Page Number)  
CLASSIFICATION

CLASSIFICATION

**C-9. Special Technical Operations Annex Format**

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

ANNEX S TO OPERATION ORDER OR PLAN (Number) (Operation  
CODEWORD) ( )  
SPECIAL TECHNICAL OPERATIONS ( )

( ) REFERENCES: List documents required for a complete understanding of the annex. References are complementary plans, publications, and Information Management systems policy documents.

Special technical operations (STO) is the organization for planning and executing compartmented capabilities. The joint staff, unified commands, and intelligence agencies all have STO organizations. They communicate through the Planning and Decision Aid System. No format is required, and specific guidance will be provided under separate cover.

ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

OFFICIAL:  
s/  
Name  
Rank and Service  
Title

(Page Number)  
CLASSIFICATION

CLASSIFICATION

## C-10. Information Management Annex Format

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

ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation  
CODEWORD) ( )

INFORMATION MANAGEMENT ( )

( ) REFERENCES: List documents required for a complete understanding of the annex. References are complementary plans, publications, and Information Management systems policy documents.

1. ( ) General. This annex provides procedures and information that must be commonly understood throughout the force for sharing, managing, fusing, and filtering critical and relevant information to facilitate decisionmaking. Much of this information is contained in other annexes of an operations order. As such, the information manager must be familiar with the operations, the assumptions, the planning guidance, and the information in the other annexes.

a. ( ) Purpose. To establish information management policies and procedures. This annex discusses the duties and responsibilities of key information management personnel such as the commander, the chief of staff, the battle staff, the command IMO, the section IMOs, and the information systems management officer. The appendices provide the detailed “how to” reference documents that discuss specific issues and details that relate to the warfighting applications of a wide audience. The intent of these appendices is to provide a unity of effort among all participants. This annex also addresses the management of common or shared processes, systems and information flow throughout the MAGTF. For each of these processes, systems, and information flows

(Page Number)

CLASSIFICATION

## CLASSIFICATION

the annex will address standards and ownership. It is through these two driving forces (standardization and ownership) that information is managed in a commonly understood manner throughout the force.

- b. ( ) Scope. Discuss the applicability of this annex.
2. ( ) Mission. State the information management mission for the overall operation. Define the broad tasks and the purpose to establish a basis for integration and coordination of actions to be taken.
3. ( ) Execution
  - a. ( ) Guiding Principles. Make maximum use of established doctrine and include the principles necessary for the coordination and guidance of all commands and agencies. Mention selected policies, doctrine, or procedures that need emphasis for guidance in the operation. State any procedures not previously published that are to be followed during the operation, as well as any authorized deviations from standard practices.
  - b. ( ) Operational Concept. Describe the operation briefly, in narrative form, emphasizing phasing and aspects of the basic plan that establish information management requirements and that affect information management capabilities and limitations. Provide OPSEC planning guidance for planning, preparing, and executing C2 functions, particularly guidance for transmission and local area network and wide area network infrastructure security planning.
  - c. ( ) Tasks and Responsibilities. In separate numbered subparagraphs for each key position, staff section, subordinate component or other subdivision of the force, assign individual information management tasks and responsibilities and include instructions that apply to that key position, staff section, component or subdivision. Consider liaison team participation as part of a multinational force to interface information management operations during multinational warfare. Use coordinating instructions in the final subparagraph to frame information management tasks and considerations common to all forces.

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

- (1) ( ) Commanding general.
- (2) ( ) Chief of staff.
- (3) ( ) Principle staff sections.
- (4) ( ) Assistant chief of staff, G-6.
- (5) ( ) Current operations cell.
- (6) ( ) Intelligence operations cell.
- (7) ( ) IMO.
- (8) ( ) Staff section/cell IMO.
- (9) ( ) Information management cell.
- (10) ( ) Subordinate command and element IMO.

d. ( ) Coordinating Instructions. Provide a separate lettered subparagraph of information regarding each coordinating instructions to frame Information Management tasks and considerations common to all forces not covered in paragraph 3.

### 5. ( ) Command and Control

- a. ( ) Command. Refer to Annex J (Command relationships).
- b. ( ) Command, Control, Communication, and Computer Systems. Refer to Annex K (Combat Information Systems).

## ACKNOWLEDGE RECEIPT

Name  
Rank and Service  
Title

(Page Number)  
CLASSIFICATION

## CLASSIFICATION

### APPENDIXES:

- 1 — Common Desktop Environment for Personal Computers
- 2 — Standard Systems, Software, and File Formats
- 3 — Commander's Critical Information Requirements Management
- 4 — Commander's Questions Management
- 5 — Battle Rhythm/Planning, Decision, Execution, Assessment Cycle
- 6 — Reports Matrix
- 7 — Track Management
- 8 — Requests for Information Management
- 9 — Suspense Log and Journal Management
- 10 — Collaborative Planning Tools
- 11 — Information Transfer
- 12 — Information Display
- 13 — Systems Integration Plan/Architecture
- 14 — Systems Protection Plan
- 15 — Skills and Training Matrix
- 16 — Exercise Design

### OFFICIAL:

s/

Name

Rank and Service

Title

(Page Number)  
CLASSIFICATION

This page intentionally left blank.

---

## Appendix D

# Information Operations Planning Tools

---

### D-1. 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 Destruction					
Deception					
Civil Affairs					
Public Affairs					

## D-2. 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.

<b>IO Planning Worksheet</b>		
Concept: _____		
COA: _____		
Objective: _____		
<b>Maneuver Endstate</b>	<b>Offensive IO Targets</b>	<b>Defensive IO Assets</b>
<b>Destruction Tasks</b>		
<b>EW Tasks</b>	<b>IO IRs</b>	
<b>PSYOP Tasks</b>		
<b>OPSEC Tasks</b>	<b>Coordination and Instructions</b>	
<b>Deception Tasks</b>		
<b>Civil Affairs Tasks</b>		
<b>Public Affairs Tasks</b>		
<b>Other Tasks</b>		

### D-3. Information Operations 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.

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

This page intentionally left blank.

---

## Appendix E

# Glossary

---

**Note:** Acronyms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official military acronyms:

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.
  2. MCRP 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*.
- 

AFIWC	Air Force Information Warfare Center
C2	command and control
C2W	command and control warfare
C3	command, control, and communications
C4	command, control, communications, and computers
CA	civil affairs
CAG	Civil Affairs Group
CCIR	commander's critical information requirement
CI	counterintelligence
CISS	Center for Information Systems Security
CNA	computer network attack
COA	course of action
COC	combat operations center
COG	center of gravity
COMSEC	communications security
DII	defense information infrastructure
DISA	Defense Information Systems Agency
DOD	Department of Defense

EA	electronic attack
EEFI	essential elements of friendly information
EP	electronic protection
EPW	enemy prisoner of war
ES	electronic warfare support
ESM	electronic warfare support measures
EW	electronic warfare
FIWC	Fleet Information Warfare Center
HN	host nation
HUMINT	human intelligence
IO	information operations
IMINT	imagery intelligence
IMO	information management officer
INFOSEC	information security
IPB	intelligence preparation of the battlespace
IR	information requirement
IW	information warfare
JCMA	Joint Communications Security (COMSEC) Monitor Activity
JFC	joint force commander
JIOC	Joint Information Operations Center
JPOTF	joint psychological operations task force
JRFL	joint restricted frequency list
JSC	Joint Spectrum Center
JWAC	Joint Warfare Analysis Center
LIWA	Land Information Warfare Agency
MAGTF	Marine air ground task force
MCPP	Marine Corps Planning Process
NACIC	National Counter Intelligence Center
NIPC	National Infrastructure Protection Center
NIWA	Navy Information Warfare Activity
NSA	National Security Agency

OPSEC	operations security
OPT	operational planning team
PA	public affairs
PSYOP	psychological operations
ROE	rules of engagement
S/EWCC	signals intelligence/electronic warfare coordination center
SIGINT	signals intelligence
STO	special technical operations
TERPES	Tactical Electronic Reconnaissance Processing and Evaluation System
USIA	United States Information Agency
VMAQ	Marine tactical electronic warfare squadron

This page intentionally left blank.

---

## Appendix F

# References

---

Joint Pub 2-0, *Doctrine for Intelligence Support to Joint Operations*

Joint Pub 2-01, *Joint Intelligence Support to Military Operations*

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

Joint Pub 2-01.2, *Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations*

Joint Pub 2-02, *National Intelligence Support to Joint Operations*

Joint Pub 3-05, *Doctrine for Joint Special Operations*

Joint Pub 3-13, *Joint Doctrine for Information Operations*

Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*

Joint Pub 3-51, *Electronic Warfare in Joint Military Operations*

Joint Pub 3-53, *Doctrine for Joint Psychological Operations*

Joint Pub 3-54, *Joint Doctrine for Operations Security*

Joint Pub 3-57, *Doctrine for Joint Civil Affairs*

Joint Pub 3-58, *Joint Doctrine for Military Deception*

Joint Pub 3-61, *Doctrine for Public Affairs in Joint Operations*

Joint Pub 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*

Joint Pub 6-02, *Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems*

Chief of Naval Operations Instruction 3430.26, “Implementing Instruction for Information Warfare/Command and Control Warfare.”

Naval Doctrine Publication 6, *Naval Command and Control Warfare*

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

US Army Field Manual 100-6, *Information Operations*

Marine Corps Order 3430.1, “Policy for Information Operations.”

Chief of Naval Operations/Commandant of the Marine Corps Memorandum “Information Warfare and Command and Control Warfare (IW/C2W).”