



HANDBOOK



15-03

FEB 15

INFORMATION OPERATIONS *Quick Reference Guide*

Lessons and Best Practices

US UNCLASSIFIED
FOR OFFICIAL USE ONLY

Handling Instructions for CALL Electronic Media and Paper Products

Center for Army Lessons Learned (CALL) authorizes official use of this CALL product for operational and institutional purposes that contribute to the overall success of U.S. government efforts.

The information contained in this product is provided for informational purposes only and is not necessarily approved U.S. Army policy or doctrine.

This product is designated for official use by U.S. government personnel and their approved contractors. It cannot be released to allies, coalition partners, or the public without the consent of CALL. This product has been furnished with the expressed understanding that it will be used for official defense-related purposes only and that it will be afforded the same degree of protection that the U.S. affords information marked "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" in accordance with U.S. Army Regulations 380-5, section 5-2. Official military personnel, civil service/government personnel, and approved contractors of the United States may paraphrase; quote; or use sentences, phrases, and paragraphs for integration into official U.S. government products or research.

However, integration of CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" information into official products or research renders them FOUO, and they must be maintained and controlled within official channels or approved contractor facilities and cannot be released to allies, coalition partners, or the public without the consent of CALL.

CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents may be placed on protected UNCLASSIFIED intranets within military organizations or units, provided that access is restricted through user ID and password or other authentication means to ensure that only properly accredited military, government officials, and approved contractors have access to CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" materials.

Regulations strictly forbid posting CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents to Army Knowledge Online or other Department of Defense (DOD) websites that do not restrict access to authorized personnel. AR-25-1, 15 Jul 2005, Army Knowledge Management and Information Technology, paragraph 6-4 n (2) (b) and DOD Web Site Administration Policy and Procedures (11 Jan 2002), Part II, paragraph 3.6.1 require appropriate mechanisms to protect sensitive information. DOD 5400.7-R, DOD Freedom of Information Act Program, September 1998, provides guidance on the release, safeguard, and unauthorized disclosure of FOUO information.

Appropriate disciplinary action may be taken against those responsible for the unauthorized release of FOUO information. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against those responsible for the release; in addition unauthorized releases by contractor personnel to unauthorized persons may warrant action relative to the contractor under the Federal Acquisition Regulation (FAR).

When no longer needed, all CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" paper products and electronic media will be shredded or destroyed using approved paper shredders or CDROM destroyers.

U.S. UNCLASSIFIED
For Official Use Only

CENTER FOR ARMY LESSONS LEARNED

SUPPORTING THE WARFIGHTER



Information Operations Quick Reference Guide

DIGITAL VERSION AVAILABLE

A digital version of this CALL publication is available to view, download, or reproduce from the CALL restricted website, <<https://call2.army.mil>>. Reproduction of this publication is welcomed and highly encouraged.

Common Access Card (CAC) or Army Knowledge Online (AKO) login is required to access the digital version.



Foreword

This Information Operations Quick Reference Guide assists U.S. Army units in planning and conducting information operations (IO). This guide is a compilation of IO tactics, techniques, and procedures (TTP) developed by 1st IO Command, 1st IO Battalion, personnel deployed worldwide in support of various military commands at different times at diverse echelons of support. This guide stresses basic principles and provides vetted processes and tools that can be used to one extent or another by all Army units.

The TTP in this guide are the product of IO subject-matter experts, practitioners, and field-support teams deployed to augment and support Army forces engaged in operations or contingency support missions worldwide. Though not prescriptive, these TTP are implementable at all echelons where IO is a prominent and significant feature of the operation. Commanders and staffs can adapt these TTP to best suit specific mission needs and situations.

Field Manual 3-13, *Inform and Influence Activities* (25 January 2013), is currently undergoing revision; in the interim this guide and the TTP included herein will serve units well to gain operational advantage through the conduct of IO. If a unit has TTP that should be considered for inclusion into this guide, submit the TTP to the Center for Army Lessons Learned or to the Information Operations Proponent Office, both at Fort Leavenworth, Kansas.

JOHN E. BIRCHER IV
COL, IO
Director, Information Operations Proponent
Office

Information Operations Quick Reference Guide	
Table of Contents	
Introduction	1
Chapter 1. Mission Analysis from an Information Operations Perspective	11
Chapter 2. Analysis of the Information Environment	21
Chapter 3. Crafting Effective Intelligence and Information Requests to Support Information Operations	25
Chapter 4. Information Operations Input to Intelligence Preparation for the Battlefield	35
Chapter 5. Staff Estimate and Orders for Information Operations	41
Chapter 6. Supporting the Commander's Narrative and Communication Synchronization	47
Chapter 7. Information Operations Working Group	53
Chapter 8. Tactical Operations Security	63
Chapter 9. Tactical Deception	71
Chapter 10. Combat Camera	79
Chapter 11. Media Analysis Within the Information Environment	85
Chapter 12. Tips for Conducting Face-to-Face Meetings	93
Chapter 13. Countering Threat Propaganda in the Information Environment	99
Chapter 14. Tactical Perception Management	105
Chapter 15. Staff Battle Drills	113
References	121

Center For Army Lessons Learned

Director	COL Paul P. Reese
CALL Analyst	Bruce D. Adams
Contributing Authors	LTC Toby W. Prudhomme, 1st Battalion, 1st IO Command Richard Simon, 1st IO Command

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

NOTE: Any publications (other than CALL publications) referenced in this product, such as ADPs, ADRPs, ARs, FMs, and TMs, must be obtained through your pinpoint distribution system.

Introduction

The Commander and the Staff

(U) Information Operations (IO) Mission

(U) Commanders broadly determine the role IO will have during current and future operations assigned to the unit. Commanders realize that integrating IO as part of operations is best understood as the integration of diverse and seemingly unrelated capabilities. Although associated with IO, those capabilities are not owned by IO. These capabilities, referred to as information-related capabilities (IRCs), are “tools, techniques, or actions that affect any of the three dimensions of the information environment” (Joint Publication 3-13, *Information Operations*). IO synchronizes IRCs employed to shape, exploit, and influence the information environment (IE). Commanders look to IO subject-matter experts (SMEs) on the staff to determine and generate the required and desired effects in those aspects of the IE most relevant to the unit’s area of operation (AO).

(U) Commanders understand that the mission of IO is to decisively affect the IE to operational advantage by synchronizing IRCs and their effects. Army views land-force IO as specialized knowledge of and ability to plan and deliver synchronized effects in the IE, which it terms IE effects — the combined, synergistic effects resulting from the synchronized employment of IRCs and their specialized effects.

(U) To accomplish the land-force IO mission, commanders, with specialized advice and support from their IO officer and staff element, perform the following:

- Visualize the IE as an operationally significant consideration within the unit’s AO.
- Visualize a comprehensive desired end state that clarifies the intended IE end state.
- State commander’s intent, clarifying desired outcomes within the IE in terms of objective effects.
- State commander’s communication strategy guidance (prevailing narrative/unifying theme).
- Ensure IO is integrated as a necessary part of the operations process.

Commander’s Intent

(U) The commander’s intent is a statement of purpose that coalesces and focuses all unit activity toward attainment of the desired end state and helps subordinates to act with disciplined initiative. Since the end state depends heavily on the effects achieved within the IE, commanders must

be explicit in their intent and subsequent guidance about addressing, not only expectations in the physical dimension, but also the informational and cognitive dimensions of the IE as well. This might include highlighting specific objectives within the IE or specifying which IRCs are best suited to meet operational requirements. It might also include articulating whether IO will be weighted toward engagement or exploitation.

(FOUO) Commander's Communication Strategy

(FOUO) The commander's communication strategy is a comprehensive approach to engaging all relevant foreign audiences in the unit's AO. Comprehensive does not mean long or complicated. The primary purpose of the communication strategy is to explain operational activities in relation to the desired end state. Commanders can do this various ways, but their strategy will typically include the following:

- A restatement of the desired end state that clarifies engagement goals.
- The preferred means used to engage audiences in the unit's AO.
- The prevailing narrative or unifying theme that aligns unit activities with the preferred words and images used to describe unit operations.
- The approved themes and messages.
- Guidance on the following:
 - Specific engagement effects.
 - Specific IRC employment.
 - Consequence management (mitigating unintended consequences).
 - Specific coordination (i.e., unified action partners).
 - Limits and constraints affecting communication and influence.

(U) Commanders rely on staff SMEs, typically IO and public affairs (PA) personnel, to develop their communication strategy. IO and PA are separate activities on the staff. Each affect and impact the IE in different, but sometimes complementary, ways. However, there are also instances when these activities give rise to potential points of overlap or friction. Commanders look to their IO and PA staffs to de-conflict and mitigate such instances beforehand, when possible, or in a timely and efficient manner as experienced.

(FOUO) Engagement and Exploitation

Engagement and exploitation are the ways through which the unit can achieve effects in the IE. These terms are not meant as absolute or restrictive; rather, the terms broadly group the types of activities units

INFORMATION OPERATIONS QUICK REFERENCE GUIDE

will undertake to achieve desired effects. Engagement involves the synchronization of IRCs in order to communicate with relevant audiences in the AO. It is generally, but not always, more human-focused and psychological and runs the gamut from persuasive to coercive. Exploitation involves the synchronization of IRCs in order to protect friendly information systems and situational awareness and, conversely, disrupt, corrupt, or usurp threat information systems and situational awareness. It is generally, but not always, more system- and data-focused and runs the gamut from passive defense to active attack. Table 1 provides examples of engagement and exploitation activities.

Engagement	Exploitation
Soldier and leader engagement (SLE), in all forms.	Electronic attack (EA) directed against threat command and control (C2) and intelligence, surveillance, and reconnaissance (ISR) in all forms.
Counterpropaganda in most forms.	Offensive cyberspace operations (CO) attack directed against threat C2 and ISR in all forms.
Civil affairs projects and/or events designed to engender support, trust, and cooperation.	Operations security (OPSEC) used to deny threat forces critical information about friendly units.
Public-Private Partnership, where the intent is to make a statement to illicit a desired behavior or perception.	Military deception (MILDEC) directed against threat decisionmakers.
Use of information to explain, defend, and advocate U.S. military force presence, actions, or objectives.	Physical destruction of threat MILDEC, C2, and ISR assets, personnel, and facilities.
Use of information to gain local support and cooperation.	Counterintelligence used to identify and out threat espionage and sabotage directed against friendly forces.
Use of polling to ascertain the perceptions and attitudes of foreign local populations.	Military information support operations (MISO) used to erode the will/morale of threat forces and hinder threat decisionmaking and C2 of its forces in all forms.

Engagement	Exploitation
Use of information to build teams and cooperation among coalition partners and allies.	Lethal force used against threat leaders and decisionmakers to disrupt, degrade, or impede threat C2 of its forces.
Use of direct marketing techniques to influence the perceptions and attitudes of foreign local populations.	Malicious corruption of threat web sites used to C2 forces, plan actions against friendly, and solicit volunteers to the cause.
	Use of information technology (IT)/IE/cyberspace to warn/dissuade local citizenry from interfering with friendly operations.
	Use of IT/IE/cyberspace to entice the local foreign citizenry to report on threat activities and to out threat agents.
	Disruption of foreign IT/IE/cyberspace to mask or deny friendly observables relevant to impending or ongoing operations.
	Disruption of foreign IT/IE/cyberspace used by threat forces and their supporters to incite the local populace against friendly operations.
	Disruption of foreign IT/IE/cyberspace to increase ambiguity among threat forces and their supporters relative to friendly unit intentions, capabilities, and vulnerabilities.
	MISO directed against threat ISR personnel reinforcing the perception that turning on ISR platforms will result in destruction of the platform and personnel manning the platform.
	MISO directed against threat MILDEC and C2 system personnel reinforcing the perception that the act of transmitting information via the MILDEC/C2 platforms will result in destruction of the transmitter and personnel manning the transmitter.

Table 1. Engagement and exploitation activities.

Information-Related Capabilities

(FOUO) IRCs are tools, techniques, or activities employed within a dimension of the IE used to create effects and operationally desired conditions (ADRP 6-0, *Mission Command*). Any capability can be information-related, if so designated by the commander. However, certain capabilities are more inherently information-related in that many deal almost exclusively with engagement or exploitation in the IE. The availability of IRCs, whether organic or attached, varies from unit to unit and level to level. Some will have an IRC representative on staff, but not the actual IRC itself. Others will have both and still others, neither. As the centralized focal point on staff for IE effects, the IO officer will assist the commander in identifying available IRCs and requesting augmentation, as required. The IO officer will also recommend IO unit augmentation, which may be provided by 1st Information Operations Command (Land) or one of the theater IO groups.

While not absolute, the following IRCs tend to be available to most units:

- Operations security (OPSEC).
- Military deception (MILDEC).
- Soldier and leader engagement (SLE).
- Physical security.
- Presence, posture, and profile.
- Physical destruction.
- PA (available to the commander, but not synchronized by IO).

The following IRCs are available based on task organization:

- Civil affairs operations (CAO).
- Military information support operations (MISO).
- Counterintelligence.
- Electromagnetic spectrum operations (EMSO).
- Electronic warfare (EW).
- Cyberspace operations (CO).
 - Defense of the network.
 - Offensive cyberspace operations.
 - Defensive cyberspace operations.

- Special technical operations (STO).
- Combat camera (COMCAM).

(FOUO) OPSEC. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations. OPSEC is designed to meet operational needs by mitigating risks associated with specific vulnerabilities in order to deny the threat critical information and observable indicators. A successfully executed OPSEC program enables operations by preventing misinformation, disinformation, and information fratricide.

(FOUO) MILDEC. Involves actions executed to deliberately mislead threat military, paramilitary, or violent extremist organization decisionmakers. The intent of MILDEC is to feed information that deliberately misleads threat decisionmakers about friendly military capabilities, intentions, and operations, leading the threat to take specific actions (or inactions) that contribute to accomplishment of the friendly mission. MILDEC consists of counter-deception, deception in support of OPSEC, and tactical deception.

(FOUO) SLE. Interpersonal interactions by Soldiers with audiences in an AO. They can occur as face-to-face encounters on the street or as scheduled meetings. Commanders lead Soldier engagement efforts and prepare subordinates for conducting these activities throughout unified land operations. A fundamental and complex duty of a land force involves Soldiers operating among local audiences. Often, audiences in an AO look, act, and think differently from Soldiers. As such, Soldiers prepare to bridge these differences to build alliances, to encourage cooperation and noninterference, and to drive a wedge between the friendly or neutral audiences and threat forces.

(FOUO) Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft. Physical security contributes directly to information protection. Information, information-based processes, and information systems — such as mission command systems, weapon systems, and information infrastructures — are protected relative to the value of the information contained and the risks associated with the compromise or loss of information.

(FOUO) Presence, Posture, and Profile. The presence of a force can have a significant effect on the perceptions of threat forces and others. Deploying even limited capability to the right place at the right time can convey to the target-friendly force commitment and determination. The posture of troops on the ground can demonstrate both commitment and intent and must be considered and balanced with the requirements of force protection. The public profile of commanders at all levels can have a huge impact on

perceptions. The public role of the commander must be carefully analyzed and opportunities used to engage important target audiences as warranted.

(FOUO) Physical Destruction. The systematic degradation or destruction of threat information, information systems, networks, and nodes in order to prevent threat forces from commanding and controlling their forces. Physical destruction has the added benefit of having a significant psychological impact on threat forces. Carefully applied force can play a major role in disrupting and deterring threat forces, thereby preventing them from achieving planned objectives.

(FOUO) CAO. Actions planned, executed, and assessed by civil affairs forces to enhance awareness of and manage the interaction with the civil component of the operational environment; identify and mitigate underlying causes of instability within civil society; or involve the application of functional specialty skills normally the responsibility of civil government.

(FOUO) MISO. Planned operations to convey selected information and indicators to foreign audiences to influence emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.

(FOUO) Counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for, or on behalf of, foreign powers, organizations, persons, agents, or international terrorist organizations or activities.

(FOUO) EMSO. Planning, coordinating, and managing the use of the electromagnetic spectrum through operational, engineering, and administrative procedures. Normally a G-6/S-6 function aligned with network operations (NETOPS), IO seeks to synchronize EMSO activities in order to optimize friendly use of the electromagnetic spectrum and enhance friendly decisionmaking through effective mission command.

(FOUO) EW. A military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack threat forces operating information-based systems in the electromagnetic spectrum. In most cases the focus for IO will be on the use of EA capabilities. EA is a division of EW, involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

(FOUO) CO. The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace is defined as a global domain within the IE consisting of the interdependent network of IT infrastructures and resident data, including the

Internet, telecommunications networks, computer systems, and embedded processors and controllers. IO also considers NETOPS activities conducted to operate and defend the Global Information Grid as an important factor associated with CO. In the case of IO, the focus is on the defense of the network and information important to friendly decisionmaking. IO works collaboratively with the G-6/S-6 to improve the defensive CO and information assurance posture of the unit.

(FOUO) STO. An option available on some staffs often employed to address staff-identified complicated or critical problem sets when traditional IRC will not successfully accomplish the desired end state. The staff requests assistance through established staff channels and procedures for planning. Currently, STO billets exist in division and higher echelons. From these echelons, these planning and execution requests can be supported and fill the gap between traditional IRC and special problem sets. When requesting integrated Joint STO (IJSTO) support, the staff focuses on the desired end state and not specific capabilities or desired effects. IJSTO support is a complicated and thorough process. It involves many agencies to develop the concept of operations and acquires access and authorization, typically an involved and lengthy process. Unless concept operations and authorizations are already established, IJSTO staffs are significantly challenged to plan for immediate, time-sensitive events.

(FOUO) COMCAM. A tool designed to provide operational imagery to support combat, information, humanitarian, special force intelligence, engineering, legal, and other military activities. COMCAM units maintain the capability to acquire, edit, disseminate, archive, manage, and transmit imagery. All COMCAM units are equipped to acquire imagery in darkness and inclement weather.

IO Element

(U) The G-3/S-3 IO element is authorized at Army formations at echelons brigade-through-theater Army. The element is embedded within the G-3/S-3 movement and maneuver cell. The former G-7/S-7 inform and influence activities section becomes the IO element. The IO element within the G-3/S-3 is the staff focal point for the conduct of IO and synchronization of IRC's information support operations (ISO). The IO element is led by an IO officer. Roles, responsibilities, and functions of the personnel assigned to the IO element broadly include planning, synchronizing, and assessing the effects of IRCs employed to generate measurable and predictable effects in the IE spanning all three dimensions: physical, information, and cognitive. The G-3/S-3 is responsible for the integration of all available unit capabilities to include IRCs through the operations process in support of higher headquarters orders and the commander's specific guidance and intent.

(U) The IO element performs the following:

- Leads the IO working group.
- Analyzes the IE to identify opportunities to employ IRCs and generate IE effects to protect, enable, and support operations (develop the combined information overlay).
- Requests intelligence support to facilitate IRC/IE effects synchronization.
- Develops the consolidated IRC/IE effects synchronization concept of support.
- Assesses the risks associated with IRC/IE effects synchronization within the AO's ISO operations.
- Assesses the effectiveness of IRC/IE effects in synchronized ISO.
- Enables realization of the commander's intent (prevailing narrative/unifying theme) through de-confliction of IRCs/IE effects, themes, and messages used during operations.
- Synchronizes IRC/IE effects employment as an integral part of operations.
- Synchronizes IRCs/IE effects in the ISO military objectives associated with the following:
 - MILDEC (from inception to termination).
 - OPSEC.
 - EW.
 - CO.
 - MISO.
 - SLE.
 - Theme and message delivery.
 - Maneuver.
 - Presence, posture, and profile.
 - Fires and physical destruction.
 - Intelligence and counterintelligence.

- Mission command and NETOPS.
- STO.

(U) The IO element, as the staff focal point for IRC/IE effects synchronization, is the entry point for external IRC and IO support assets and resources. The IO element oversees the integration of these external assets and resources into the overall IRC/IE effects planning, implementation, and assessment process. In many cases, the Army deploys specialized teams of IRC and IO SMEs to support units in the field that can include IO field support teams, MILDEC planning and support teams, vulnerability assessment and OPSEC support teams, and CO support teams.

(U) IO Support Team. Certain Army units deploy specialized teams of IRC and IO SMEs to support units in the field. Such teams can include IO field support teams, MILDEC planning and support teams, and vulnerability assessment and OPSEC support teams. These teams deploy to augment existing staff expertise and assist the staff in the planning, synchronizing, and assessing the employment of IRCs in support of operations.

(U) CO Support Team. Certain Army units deploy specialized CO SMEs to support units in the field. These SME teams deploy to augment existing staff expertise and assist the staff in planning, synchronizing, and assessing CO in support of operations.

Chapter 1

Mission Analysis

from an Information Operations Perspective

This chapter describes the following:

- How to apply mission analysis to planning of an information operation (IO).
- Techniques to adapt mission analysis to the needs of the IO staff.

This planning aid, designed to augment doctrine, is based on the tactics, techniques, and procedures' pre-deployment training of the 1st Information Operations Command (Land).

(U) IO and Mission Analysis

As part of the planning process, the IO staff must conduct its own mission analysis.

MDMP Step	IO Focus
Analyze HHQ Order	Analyze HHQ info operation
Perform IPB	Define IE & determine threat COAs in the IE (See 1st IO Cmd Info IPBaid)
① Determine Tasks	Determine what IO must do
② Review Available Assets	Determine organic & supporting IO capabilities
③ Determine Constraints	Determine constraints on info content & flow
④ Identify Facts & Assumptions	Facts & assumptions relevant to info content, flow & use
⑤ Perform Risk Assessment	Input hazards resulting from IO tasks
⑥ Determine CCIR & EEFI	Determine Essential Elements of Information (EEFI)
Determine ISR Plan	Input IRs for IO
Update Timeline	Input lead time for IO tasks
Write Restated Mission	Write IO support to mission statement (if used)
⑦ Deliver Msn Analysis Briefing	Input to mission analysis briefing
Approve Restated Mission	Approve IO support to mission statement
Develop Cdr's Intent	Input to Commander's Intent
Issue Cdr's Guidance	Guidance for IO
Issue Warning Order	Input for IO
Review Facts & Assumptions	Address changes to IO planning factors

Figure 1-1. MDMP

(U) Mission Analysis Worksheet

- The worksheet is a tool to conduct mission analysis.
- It focuses on the minimum information needed for a plan.
- The format (see Table 1-1) follows the sequence of the mission analysis briefing format, not the steps of mission analysis.

1. Facts:
2. Assumptions:
3. Tasks:
4. Constraints:
5. Available Assets:
6. Risk Assessment:
7. Commander's Critical Information Requirement: a. Priority Information Requirements (PIR) b. Friendly Force Information Requirements (FFIR)
8. Essential Elements of Information (EEFI):

Table 1-1.

(U) Determine Tasks

- Tasks generally identify what must be accomplished in order to exploit threat forces, engage foreign audiences, and protect friendly information-related capabilities (IRCs) in the area of operations:
 - Determine objectives and operational advantage.
 - Identify specified and implied IRC synchronization tasks, not tasks to individual capabilities. Individual capability tasks will be developed by the capability manager in response to the broader IO concept of support.
 - * Specified tasks are tasks specifically assigned to a unit by its higher headquarters.
 - * Implied tasks are tasks that must be performed to accomplish a specified task or the mission, but are not stated in the higher headquarters' order.

- Identify staff coordination, administrative, or SOP tasks (i.e., conduct a weekly IO working group or submit daily reports).
- Organize specified and implied tasks to improve clarity:
 - Tasks to shape the information environment (IE) through actions designed to affect the flow and content of information known to have a predictable influence on military operations.
 - Tasks to engage foreign audiences.
 - Tasks to exploit threat forces' command and control, information and intelligence gathering, and leadership and decisionmaking.
 - Tasks to protect friendly mission command and decisionmaking.
- Essential tasks are specified or implied, and must be executed to accomplish the mission. Select three to five essential tasks.

(U) Review Available Assets

- Examine assets to determine IRC and Army-unique IO unit capabilities and limitations.
- Consider organic and supporting assets based on task organization, support relationships, and status of units.
- Compare assets to specified, implied, and essential tasks to determine if there are enough assets to accomplish all tasks.

Example Asset List for IO					
Organization	Asset	Means	Supported Essential Task	Effect	Target
Organic Assets					
Supporting Assets					

Table 1-2.

(U) Determine Constraints

- Constraints are restrictions on the use and employment of IRCs.
- There are two types of constraints:
 - Prohibited actions (cannot do).
 - Directed actions (must do).
- Affect the employment of IRCs.
- Organize by effect on information content and flow.

Info Content	<ul style="list-style-type: none"> • Avoid themes that favor any ethnic group • Stress themes that highlight cooperation • PSYOP product approval by Div Cdr • Deception approval by Div Cdr
Info Flow	<ul style="list-style-type: none"> • No cross-boundary electronic attack • All EA must be coordinated with the JRFL • US PSYOP products may not be disseminated by non-U.S. allies • Public Affairs posture is Passive • Mosques are on the restricted target list • Combat camera priorities

Figure 1-2. Example of constraints for IO.

(U) Identify Facts and Assumptions

- Facts and assumptions establish an understanding of the situation:
 - **Facts.** Known data concerning the situation.
 - **Assumptions.** Accepted as true in absence of facts.
- Focus on facts and assumptions that concern assigned tasks.
- Organize by IE (information content and flow), threat capabilities and vulnerabilities in IE, and friendly capabilities and vulnerabilities in IE.

Example Facts & Assumptions	
IE	<ul style="list-style-type: none"> • Local populace is illiterate (F) • Radio primary means to reach populace (F) • Populace is pro-U.S. (F) • Local Leaders can control populace behavior (A)
Threat Forces	<ul style="list-style-type: none"> • SIGINT is limited to short range VHF radio • Use satellite and cell phones for C2 (F) • Will direct propaganda against U.S. forces (A)
Friendly Forces	<ul style="list-style-type: none"> • Friendly forces can jam the threat's C2 • Friendly forces can use local radio stations (A)

Figure 1-3. Example of facts and assumptions.

(U) Perform Risk Assessment

- Identify and assess risks in the IE arising from the essential tasks for IO.
- The first two steps of risk assessment are accomplished during mission analysis.

- Identify two kinds of hazards (risk):
 - Tactical risk is concerned with hazards that exist because of the presence of the threat.
 - Accidental risk includes risks to friendly forces, civilians, and the operation’s impact on the environment.

Essential Task	1 Identify Hazards	2 Assess Hazards	3 Develop Controls	4 Determine Residual Risk	5 Implement Controls

Table 1-3. Essential task risk assessment.

(U) Input to Commander’s Critical Information Requirements (CCIRs)

The CCIR identifies the information needed to direct execution of the mission. Two types of a CCIR are a priority intelligence requirement (PIR) and a friendly force information requirement (FFIR):

- The PIR includes the following:
 - Information the commander must know about the threat.
 - For IO, PIRs focus on conditions in the IE and threat actions that affect the IE.
- The FFIR includes the following:
 - Information the commander must know about the friendly force.
 - For IO, FFIRs focus on friendly force capability to shape information content and flow.

(U) Essential Elements of Information (EEFI)

- EEFI is information that must be protected from the threat’s intelligence system.
- Sources of information for developing EEFI include the commander’s guidance; facts, assumptions, and essential task lists; and the intelligence estimate (adversary intelligence capabilities and requirements).
- Write EEFI as statements, not questions.

Example of CCIR & EEFI for IO	
PIR	<ul style="list-style-type: none"> • What info systems is the adversary using for C2? • What means is the enemy using to disseminate propaganda? • Is adversary propaganda turning popular opinion against operations?
FFIR	<ul style="list-style-type: none"> • Media coverage of alleged friendly force's misconduct • Civilian casualties caused by friendly force operations
EEFI	<ul style="list-style-type: none"> • Friendly force's means of intelligence collection • Tribal leaders who are assisting friendly forces

Figure 1-4. Example of CCIR and EEFI for IO.

(U) Mission Analysis Briefing

The IO part of the briefing is either included in the G-3 and G-2 planners’ presentations or, when appropriate, developed as separate slides. IO input typically includes the following:

- **Mission.** Commander’s narrative and intent for IO of headquarters two levels up and relevant commander’s IO guidance.
- **Intelligence Preparation of the Battlefield.** Combat intelligence officer and enemy courses of action in the information environment.
- **Facts and Assumptions.** Critical facts and assumptions for IO.
- **Tasks.** Specified, implied, and essential tasks for IO.
- **Constraints.** Restrictions affecting the use and employment of IRCs.
- **Forces Available.** Organic and supporting IO-capable assets and its capabilities and limitations.

- **Risk Assessment.** Risks in the IE.
- **CCIR.** Input to PIR and FFIR.
- **Time Line.** Input to the time allocation plan for accomplishment of IO essential tasks.
- **Restated Mission.** IO mission statement (if used).

Chapter 2

Analysis of the Information Environment

This chapter provides the following information:

- How to use center of gravity (COG) analysis to identify adversary capabilities, requirements, and vulnerabilities in the information environment (IE).
- Techniques to determine exploitable adversary vulnerabilities in the IE.

This chapter is designed to augment doctrine, based on the tactics, techniques, and procedures of the pre-deployment training of the 1st Information Operations Command (Land).

(U) Threat COG Analysis and the Military Decision Making Process

COG analysis is conducted during mission analysis of the Military Decisionmaking Process (MDMP). COG analysis supports by the following:

- Evaluating the threat’s critical vulnerabilities for exploitation.
- Identifying high pay-off targets.

The G-2/S-2 routinely provides a general COG analysis of the threat. The information operations (IO) element refines the COG analysis with IE-related details that enable a more complete analysis and understanding of threat intentions, capabilities, and vulnerabilities in the IE.

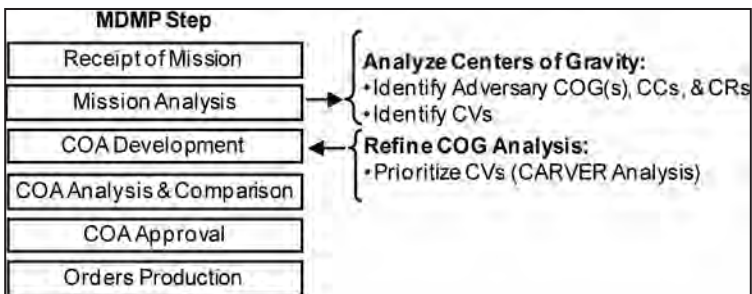


Figure 2-1. Analyze and refine COGs in the MDMP.

(U) COG Analysis Hierarchy

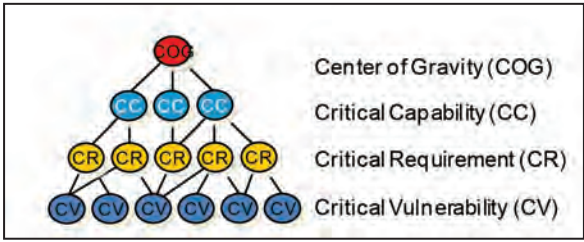


Figure 2-2. COG analysis is portrayed as a pyramidal hierarchy.

- **COG.** A source of strength, power, and resistance.
- **Critical Capabilities (CCs).** These are the primary capabilities (functions) a COG must possess in order to operate.
- **Critical Requirement (CR).** Those resources, systems, and means that the threat requires to perform its critical capabilities.
- **Critical Vulnerability (CV).** A weakness in a CR that allows it to be exploited.

(FOUO) COG Analysis Steps

- **Identify Threat COGs.** Visualize the threat as a system of systems. Determine which component of the system is so vital the system cannot function without it. A COG may be either a tangible entity or an intangible concept.

Validity Test: Will the destruction, neutralization, or substantial weakening of the COG result in changing the adversary’s course of action or denying its objective(s)?

- **Identify CCs.** Analyze the COG to determine what primary abilities (functions) the threat possesses. The functions are often standard support functions, such as “communicate” and “sustain.” CCs are not tangible objects, but rather adversary functions.

Validity Test: Is the CC directly related to the function of the COG? Is the identified CC necessary for the COG to function?

- Identify CRs. Each CC is analyzed to determine what conditions, resources, or means enable threat functions or mission.
NOTE: CRs are tangible elements such as communications means, weapons systems, or even geographical areas or terrain features. CRs are tangible elements of the adversary organization.

Validity Test: Will the absence or loss of the CR disable the threat's CC? Can the CR be nominated to the high-value target list? Does the threat consider the CRs to be critical?

- Identify CVs. Each CC is analyzed to determine which threat CRs, or components thereof, are vulnerable to neutralization, interdiction, or attack. CVs can be either physical structures and equipment or cognitive characteristics.

Validity Test: Will exploitation of the CV disable the associated CR? Does the friendly force have the resources to affect the identified CV?

- Prioritize CVs. Criticality, accessibility, recuperability, vulnerability, effect, recognizability (CARVER) is a methodology used to prioritize targets. Apply the following CARVER criteria against each CV to determine impact on the threat organization and friendly mission accomplishment.

- **Criticality.** How important to the threat is the CV? How will its disruption or destruction impact threat operations?
- **Accessibility.** Is the CV accessible to the friendly force in time and space? Can the friendly force actually get at the target?
- **Recuperability.** How much effort, time, and resources will the threat expend to reconstitute the CV?
- **Vulnerability.** Is the CV exposed to friendly force action?
- **Effect.** Will the intended effect(s) be achieved by striking the CV?
- **Recognizability.** Can the CV be identified by the friendly force for engagement and assessment?

(U) CARVER Process

Critical Vulnerability	C	A	R	V	E	R	Value Total	
	4	2	1	3	4	5	19	Priority 1
	2	2	4	3	5	5	21	Priority 2
	3	3	2	1	5	4	18	Priority 3
	1	5	3	2	3	4	15	Priority 4

Figure 2-3. Charting the CARVER process.

- Place CVs in Column 1.
- For each CV, assign a numerical rating from 1 to 5, which represents the outcome that targeting the CV would have on the threat. The number 5 indicates a desirable rating (from the attacker’s perspective), while the number 1 reflects an undesirable rating (again, from the attacker’s perspective) .
- Sum the values across the columns; rank order the CVs according to score.
- The rank order should be taken into consideration with resource and operational limitations to prioritize CVs into effective targets.

(U) COG in the IE

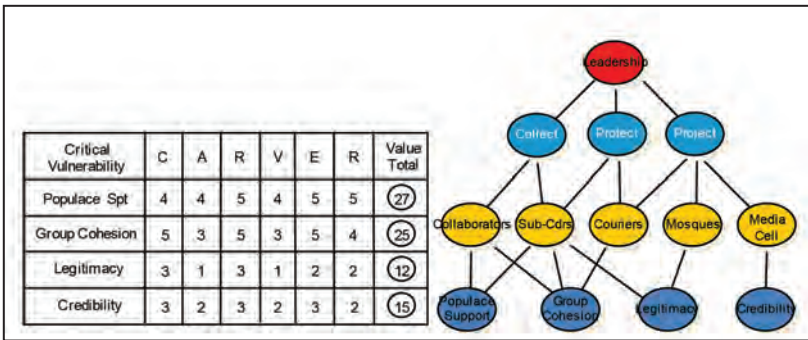


Figure 2-4. A notional example for an irregular force.

Chapter 3

Crafting Effective Intelligence and Information Requests to Support Information Operations

This chapter provides the following information:

- The information and intelligence needed to plan and execute an information operation (IO).
- Possible sources of information and intelligence for IO staffs.
- Information based on the tactics, techniques, and procedures of pre-deployment training of the 1st Information Operations Command (Land) to augment doctrine.

(U) Intelligence Support to IO

(U) General

Planning and execution of IO require both information and intelligence about threat forces and the information environment (IE). Coordination with the intelligence staff can generate the intelligence needed to understand the threat and the IE. However, as a staff element, with its own specialized needs, the IO staff must be prepared to gather information and intelligence from other sources.

(U) Terms

Information. Facts, data, or instructions in any medium or form; the meaning that a human assigns to data by means of the known conventions used in its representation. (JP 1-02)

Intelligence. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. (JP 1-02)

(FOUO) Information Intelligence Preparation of the Battlefield Overview

For staff elements, such as IO, most intelligence requirements are generated as part of the intelligence preparation of the battlefield (IPB) process. Two broad categories of information needed by the IO staff are IE and threat operations in the IE.

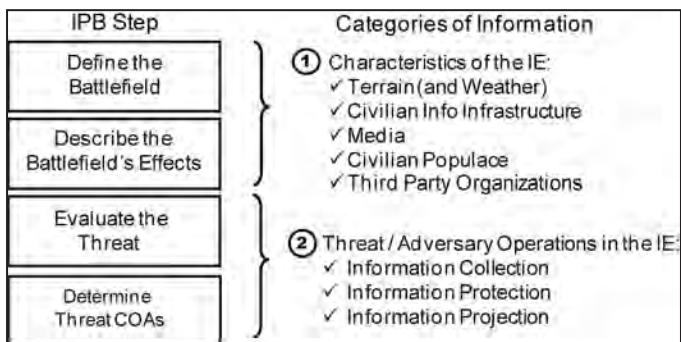


Figure 3-1. Categories of information for the IPB process.

(FOUO) Characteristics of the Information Environment

To analyze the IE, information is needed on the following significant characteristics of the area of operations (AO) and area of interest:

- **Terrain (and Weather).** Those aspects that impact information content and flow (e.g., compartmentalization, canalization, technical limits on information system employment).
 - How do terrain and weather canalize or compartmentalize information content and flow?
 - How does terrain (and weather conditions) impact information flow?
- **Civilian Information Infrastructure.** Those info systems that move information.
 - What are the key information systems? (i.e., telephone, microwave, Internet, etc.)
 - What information content is passed on each information system?
 - Who (i.e., friendly forces, threat, civilian populace) uses each information system?
 - Who manages or controls the information systems?
- **Media.** The media are a primary characteristic of every IE.
 - What media sources are present in the operating area and area of interest?
 - What information is reported by each media source?

- Who is each media's audience?
- What is the context or bias of the media outlets?
- **Civilian Populace.** Address the populace as a network of groups.
 - How does the populace communicate?
 - What information content does the populace need/want?
 - What are the populace's biases?
 - What is the populace's social organization?
 - What are the populace's cultural characteristics?
- **Third Party Organizations.** Non-government, private and international organizations (i.e., non-governmental organizations [NGOs], private voluntary organizations [PVOs], and international organizations) are competing influences in the IE.
 - What are the NGOs/PVOs/international organizations in the AO?
 - What are the organizations' purposes and objectives?
 - What information do these organizations project into the AO?

NOTE: Depending on the mission and operating environment, there may be primary characteristics of the IE other than those listed here.

(FOUO) Combined Information Overlay

The combined information overlay (CIO) is the product that provides the IO staff with visualization of the IE.

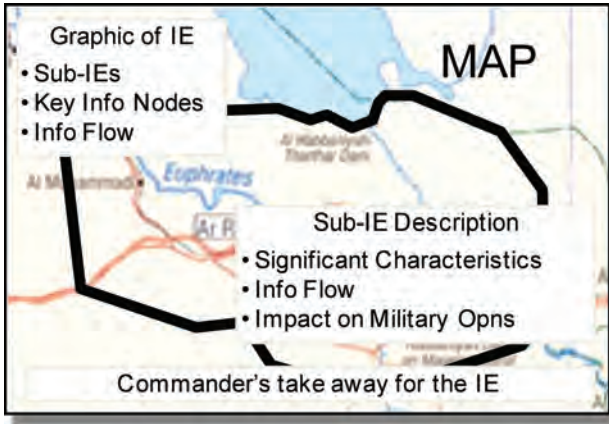


Figure 3-2. Overlay visualization of the IE.

Template for a CIO

The CIO requires information and intelligence to perform the following:

- Identify sub-IEs and key information nodes.
- Provide insight into information content and flow in the operating area.

(FOUO) Threat/Adversary Operations in the IE

Threat operations in the IE can be analyzed in terms of information collection, protection, and projection. Identify threat capabilities and vulnerabilities in the IE by performing the following:

- Collect.
 - What information does the threat need?
 - What information systems does the threat use to collect information?
 - Who are the key leaders?
 - How does the threat make decisions?
- Protect.
 - What information must the threat protect?
 - What means does the threat have?

- Project.
 - How does the threat communicate decisions?
 - What information (themes) does the threat project?
 - What capabilities and means are used?

(FOUO) IO Capability Intelligence Requirements

IO and supporting information-related capabilities (IRCs) have overlapping and competing intelligence requirements. In broad terms, IRC employment is best enabled by very specific information and intelligence, such as the following:

- Operations security.
 - Threat intelligence collection capabilities.
 - Threat intelligence requirements.
- Military deception.
 - Threat leaders' profiles.
 - Threat leaders' perceptions and biases.
- Electronic warfare.
 - Threat electronic order of battle.
 - Threat electronic nodes and systems.
- Military information support operations.
 - Threat propaganda activities.
 - Populace demographics, beliefs, and perceptions.
 - Local media.
- Civil-military operations.
 - Local populace demographics.
 - Civil government.
- Public affairs.
 - Local, regional, and international media.
 - Media bias.

(FOUO) Intelligence Resources

Organization and product intelligence resources the unit can request are listed in Table 3-1.

Organization	Products
Supported Command/Higher Headquarters	<ol style="list-style-type: none"> 1. Current Image, Human, and Signal Intelligence 2. Intelligence Summaries and Operations Reports
Marine Corps Information Operations Center	<ol style="list-style-type: none"> 1. Intelligence Preparation of the Battlefield Products 2. Assessment
4th Military Information Support Group	Regional and Special Military Information Support Operations Studies
Marine Corps Intelligence Activity	<ol style="list-style-type: none"> 1. Country Studies 2. Cultural Information
Joint Warfare Analysis Center	Node and Link Analysis
Defense Intelligence Agency	<ol style="list-style-type: none"> 1. Human Factor Analysis 2. Force Analysis and Assessment 3. Regional and Country Summaries
Other Agencies	<ol style="list-style-type: none"> 1. Node and Link Analysis 2. Leadership Profiles 3. Local and Regional Perceptions

Table 3-1. Organization and product intelligence resources.

(U) Public Information Sources

Useful public information is available on the Internet. Internet sources provide background information for situation awareness and can frequently fill specific information requirements about the media and local populace. Websites to monitor include the following:

- Media web pages.
- Public (government) web pages.
- Academic web pages.
- Social media.

As with all open-source information, it is important to evaluate the reliability and motivations of each website’s owner. Two good government sources for public information are listed in Table 3-2.

Organization	Products
DNI Open Source Center	Foreign media topics and themes
State Department	Current political issues Presidential speeches Talking points

Table 3-2. Government sources for public information.

(U) Requests for Information

Requests for information (RFIs) are used to request specific information and intelligence. Each command has its own RFI format and procedures, such as the one in Table 3-3.

INTELLIGENCE REQUIREMENTS FOR EXECUTION
Date Submitted:
Requesting Staff Section:
Subject: (Enemy or operating environment?)
Information Requirement: (Clearly state the information requirement; be specific.)
Justification: (Purpose of the request.)
Sources Checked: (Identify key products and agencies searched.)
Latest Time Information is of Value (LTIOV): (Impact on planning vs. impact on operations.)

Table 3-3. Example RFI for intelligence requirements for execution.

During execution of the operation, the IO element requires the following two broad categories of intelligence:

- Changes in the IE affecting information content and flow.
 - Changes in the information infrastructure.
 - Media reporting.
 - Rumors and disinformation.
 - Populace actions and activities.
 - Third-party organization activities.

NOTE: What has changed? How is it affecting the operation?
- Threat operations in the IE to collect, project, and protect information.
 - Threat activity in the IE directed against friendly operations.
 - Indicators that validate (or do not validate) the threat course of action.

- Threat impact and effectiveness in the IE.
- Friendly IO impact on threat forces.

NOTE: What is the threat doing in the IE? How effective is it?

Chapter 4

Information Operations Input to Intelligence Preparation of the Battlefield

This chapter provides the following information:

- How to use intelligence preparation of the battlefield (IPB) to analyze the threat and information environment (IE) in a specific geographic area.
- Techniques to visualize the impact of the IE and identify threat capabilities and vulnerabilities in the IE.

Information in this chapter is based on the tactics, techniques, and procedures of pre-deployment training of the 1st Information Operations Command (Land) to augment doctrine.

(FOUO) Overview

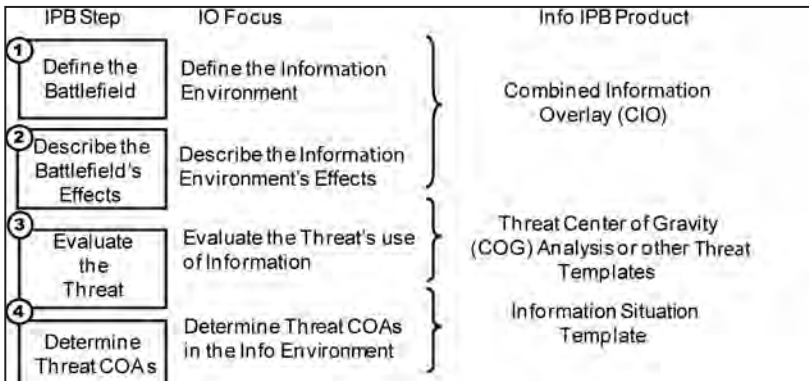


Figure 4-1. IPB steps with information operations focus.

(FOUO) Information Environment

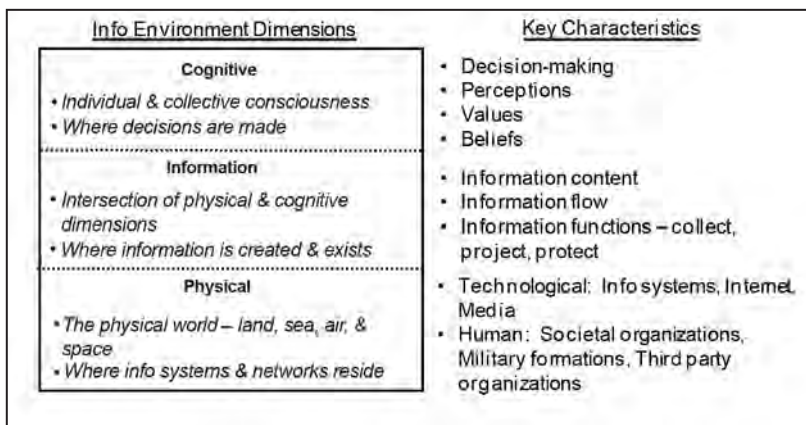


Figure 4-2. IE dimensions and key characteristics.

(U) Define the Information Environment

- Identify significant characteristics of the IE in terms of the physical, information, and cognitive dimensions.
 - Terrain and Weather. Canalization and compartmentalization.
 - Civilian Information Infrastructure. Key links, information systems, and nodes.
 - Media. Radio, television, print, and Internet.
 - Civilian Population. Demographics such as distribution, language, religion, ethnicity, and education; cultural factors such as societal structures, ideologies, perceptions, and beliefs.
 - Third Party Organizations. Non-government, private, and criminal.
 - Level of war:
 - * Tactical:
 - ◆ Physical. Terrain and weather, local information systems, and face-to-face contact.
 - ◆ Information. Line-of-sight flow: content = immediate needs.
 - ◆ Cognitive. Immediate perceptions.

* Operational:

- ◆ Physical. Regional information systems.
- ◆ Information. Over-the-horizon flow: content = higher-level issues and concepts.
- ◆ Cognitive. Near-term perceptions.

* Strategic:

- ◆ Physical. Long-distance information systems.
- ◆ Information. Global flow: content = ideas, ideologies, and philosophies.
- ◆ Cognitive. Long-term beliefs.

- (U) Describe the IE's effects.

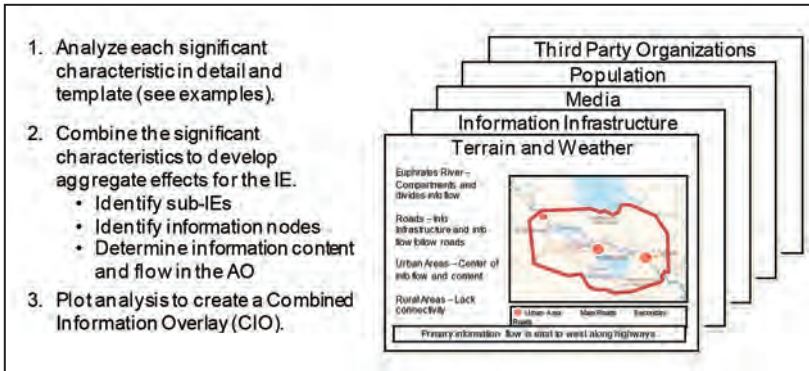


Figure 4-3. Illustrating IE effects.

○ (U) Sub-IEs and Key Nodes.

- * By identifying and acting on key nodes, a military force can affect the IE.
- * Sub-IEs are areas in which characteristics and effects are different from adjacent areas. Sub-IEs may include:
 - ◆ Physical features and cognitive aspects of the IE.
 - ◆ Areas formed by interactions of physical and cognitive dimensions.
 - ◆ Areas advantageous to either the friendly or adversary force.

* Key terrain is in the form of information nodes. Information nodes are places, persons, or infrastructure that create or transmit information. Information nodes include the following:

- ◆ Exist in each sub-IE.
- ◆ Can be human or technological, or both.
- ◆ Are located at the center of information content and flow.
- ◆ Provide an advantage to one side or the other.
- ◆ Example: Mosque with an influential Imam, key market.

○ (FOUO) Combined Information Overlay (CIO). The CIO is a graphic depiction of where and how the IE's effects will impact military operations.

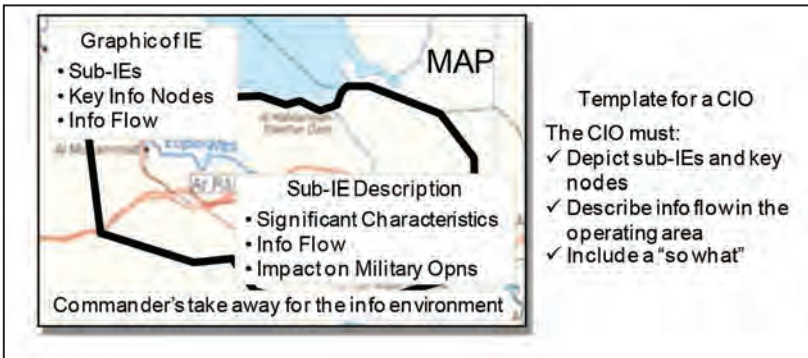


Figure 4-4. Overlay graphics of IE.

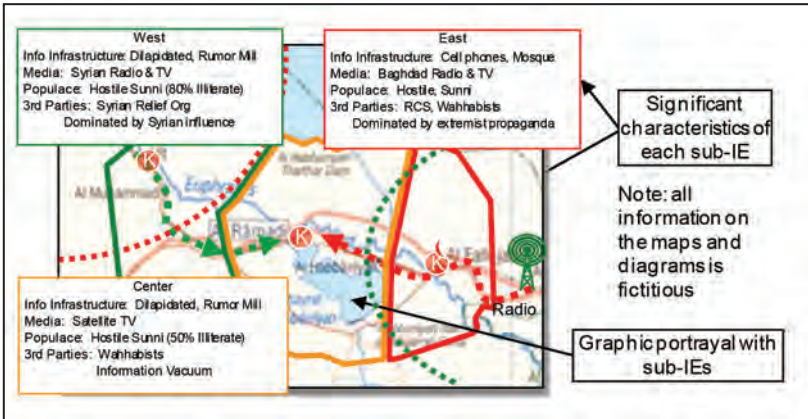


Figure 4-5. Example CIO.

- (FOUO) Evaluate the Threat with COG. A COG analysis can be used to identify threat capabilities, requirements, and vulnerabilities in the IE.

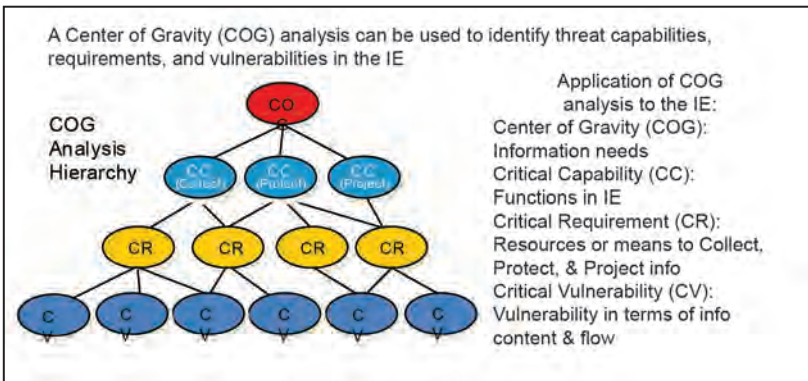


Figure 4-6. COG analysis hierarchy.

- (FOUO) Evaluate the Threat with Templates.
 - Formal modeling produces templates that portray the normal or doctrinal (historical) composition and organization of the threat's information system and its assets.
 - The result should identify threat capabilities and vulnerabilities under ideal conditions in the IE.

NOTE: Templates will vary widely by operation. The examples presented in this handbook are illustrative only.

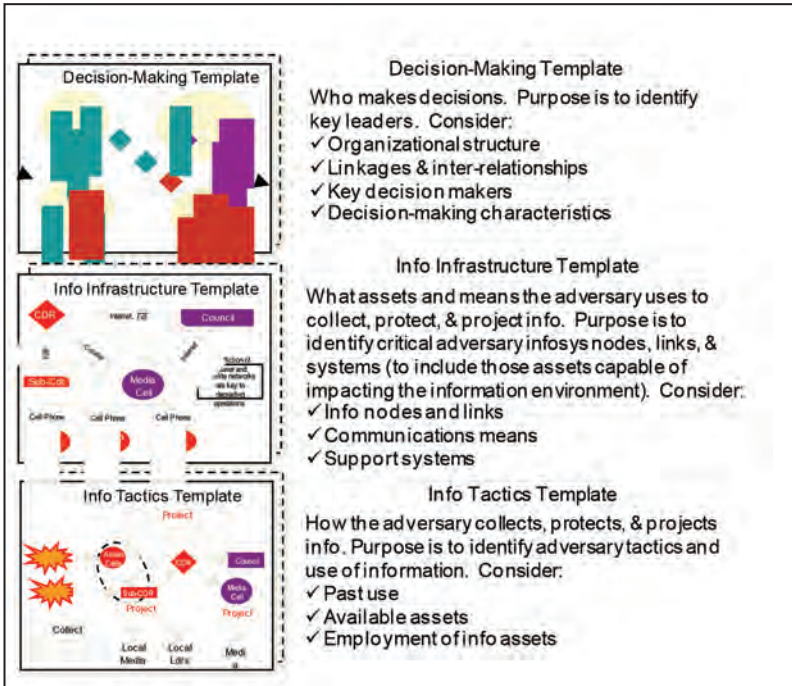


Figure 4-7. Example templates.

- (FOUO) Determine Threat Activities in the IE.

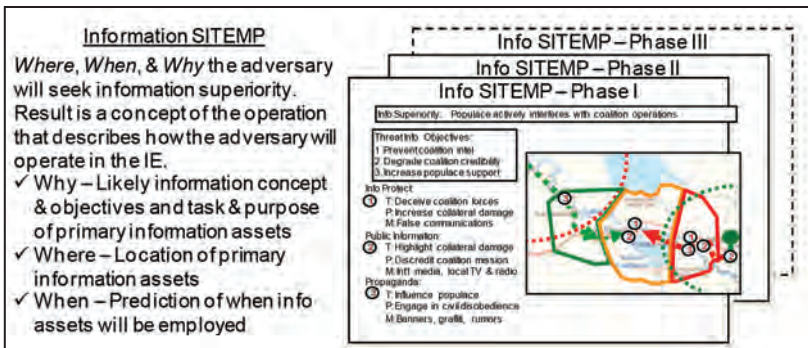


Figure 4-8. Information situation template.

Chapter 5

Staff Estimate and Orders for Information Operations

This planning aid provides the following information:

- The benefit of a staff estimate in planning information operations (IO).
- Possible formats for written and graphic IO estimates.

This chapter is based on the tactics, techniques, and procedures of pre-deployment training of the 1st Information Operations Command (Land) and is designed to augment doctrine.

(U) The Staff Estimate

The IO staff estimate is a running assessment of the situation and an analysis of the courses of action (COAs) a commander is considering. It includes an evaluation of how factors in a staff section's functional area influence each COA and includes conclusions and recommendations. Staff estimates are:

- Normally text documents, but may be formatted as maps, graphics, or charts.
- Comprehensive as possible, yet not overly time-consuming.
- Developed as part of the planning process.
- Updated as the operation progresses.

The staff estimate for IO is an estimate tailored to the specific needs of the IO staff. It assesses the situation in the information environment (IE) and analyzes the best way to achieve information superiority.

- Focus on the IE and the use of information by threat and friendly forces.
- When possible, has graphics to illustrate the less tangible aspects of IO.

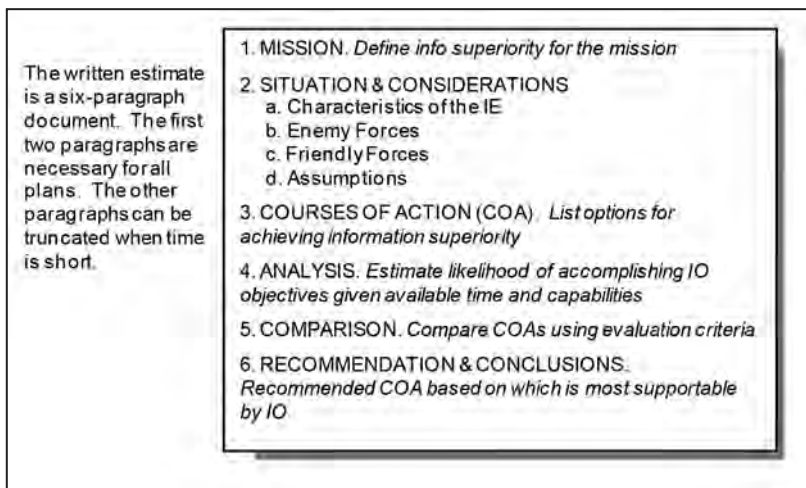


Figure 5-1. Written IO staff estimate.

(U) Mission, Situation, and Considerations

- **Mission.** Describe the operational advantage that IO actions will achieve in support of the unit mission.
- **Characteristics of the IE.** Describe the significant characteristics of the IE in terms of the physical, information, and cognitive dimensions. Consider the following characteristics:
 - Terrain.
 - Civilian information infrastructure.
 - Media.
 - Civilian population.
 - Third-party organizations.

NOTE: See the 1st IO Command information intelligence preparation of the battlefield aid for more information.

- Describe the character of each sub-IE in the AO and whether it favors friendly or threat forces.
- Identify information nodes in each sub-IE (i.e., places, persons, or infrastructure that shape information content and flow by creating or transmitting information).

- **Enemy Forces.** Describe how, when, where, and why the threat force operates in the IE. Identify threat capabilities and vulnerabilities in the IE in terms of the following:
 - Information collection.
 - Information protection.
 - Information projection.

NOTE: When possible, include likely objectives and activities in the IE.
- **Friendly Forces.** Describe friendly force capabilities to operate in the IE. Identify friendly vulnerabilities to threat and third-party actions in the IE.
- **Assumptions.** List the assumptions essential for planning, execution, and assessment of the information operation. Organize by the following:
 - IE (information content and flow).
 - Adversary capabilities and vulnerabilities in IE.
 - Friendly capabilities and vulnerabilities in IE.

(U) Graphic IO Staff Estimate

A graphic estimate contains the same basic information as a written estimate.

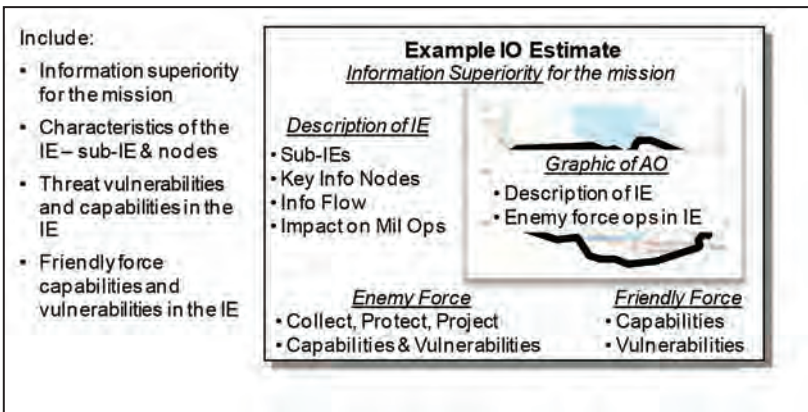


Figure 5-2. Example IO estimate.

(U) IO Appendix 15 to Annex C, Operations

Appendices are as detailed as time permits. Format can run the gamut from a series of overlays with written comments to voluminous documents.

Whatever the format, an appendix must be clear, concise, and useful to the implementing commands and units.

Appendix 15, IO describes how IO will support and enable unified land operations. The appendix illustrates and describes aggregate IO effects in the IE designed to support and enable unit operations. The primary purpose of the IO appendix is to provide the following:

- Operational details on the synchronized employment of information-related capabilities (IRCs).
- Tasks that need to be undertaken in order to achieve predictable effects in the IE.
- Information needed to assess the synchronized employment of IRC's information support operations.

Possible example formats for an IO appendix include the 5-paragraph format, matrix, or graphic.

(U) Written IO Appendix

<p>A written annex is used when:</p> <ul style="list-style-type: none"> • Time is available • Directed by G3/S3 or Unit SOP <p>Format follows a five-paragraph structure</p> <p>Depending on the command or unit, a mission statement may not be necessary</p>	<ol style="list-style-type: none"> 1. SITUATION <ol style="list-style-type: none"> a. Area of Operations b. Enemy Operations in the IE c. Friendly Capabilities and Vulnerabilities in the IE d. Civil Considerations e. Attachments and Detachments 2. MISSION. <i>IO Mission Statement (If used)</i> 3. EXECUTION <ol style="list-style-type: none"> a. Concept of Support. <i>Describe how the information operation will be conducted. Define info superiority</i> b. Assessment c. Tasks to Staff & Subordinate Units d. Coordinating Instructions 4. SUSTAINMENT 5. COMMAND & SIGNAL. <i>Arrangements needed to exchange info among IO elements</i>
--	---

Figure 5-3. Written (5-paragraph) example.

(U) Matrix IO Appendix

<p>A matrix annex is typically used when:</p> <ul style="list-style-type: none"> • Time is limited • Directed by G3/Unit SOP <p>Matrix annexes have the same elements of information as written annexes</p> <p>Text is reduced to bullet comments</p>	Example IO Annex	
	ENEMY SITUATION:	FRIENDLY SITUATION:
	MISSION:	INFO SUPERIORITY:
	CONCEPT OF SUPPORT:	
	IO OBJECTIVES / TASKS:	ASSESSMENT:
	COORDINATING INSTRUCTIONS:	
	SUSTAINMENT:	
	COMMAND AND SIGNAL:	
	APPENDICES: <input type="checkbox"/> OPSEC <input type="checkbox"/> MISO <input type="checkbox"/> MILDEC <input type="checkbox"/> EW	

Figure 5-4. Matrix example.

(U) Graphic IO Appendix (aka CONOP)


<p>A graphic annex is typically used when:</p> <ul style="list-style-type: none"> • Time is limited • Graphics are needed to clarify the operation <p>A graphic IO annex is a concept of the operation (CONOP) slide</p>	Example IO CONOP	
	<p><u>EXECUTION</u></p> <ul style="list-style-type: none"> • Info Superiority • IO Objectives • Tasks • Target Audiences • Assessment 	 <p>Map of AO</p> <ul style="list-style-type: none"> • Timeline • Constraints • Risk Assessment • Measures of Effectiveness

Figure 5-5. Graphic example.

(U) Execution Matrix

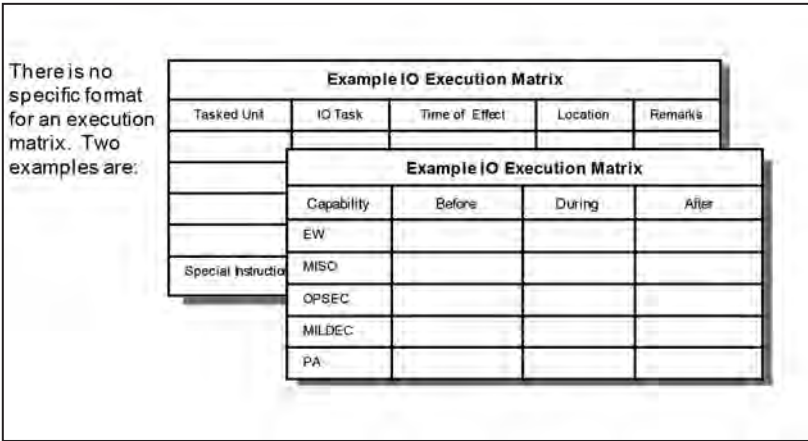


Figure 5-6. Execution matrix example.

Chapter 6

Supporting the Commander's Narrative and Communication Synchronization

This chapter provides information about how the staff can develop themes and messages in support of tactical operations when no military information support operations (MISO) or other pre-approved themes are available to support unit operations.

This chapter is designed to augment doctrine, based on tactics, techniques, and procedures of pre-deployment training of 1st Information Operations Command (Land).

(U) Themes and Messages

- Themes and messages are two distinct entities. Each has its own purpose; the two are not interchangeable.
- Themes are planning tools that guide the development of messages and other information products (e.g., talking points, MISO print, and broadcast products). Themes provide the following:
 - Represent the broad idea desired to influence the target foreign audience.
 - Are not communicated to the target foreign audience; that is the role of messages.
 - Are broad and enduring. Themes change infrequently.
- Messages contain the information that will be delivered to the target foreign audience. Messages provide the following:
 - Convey the theme to the target foreign audience.
 - Are tailored to specific foreign audiences.
 - Are meant to elicit or prevent a certain behavior.
 - Constantly change with the situation and mission.

NOTE: By doctrine, information operations (IO) is not responsible for the development of themes and messages; however, commanders may direct IO elements to assist in the development of themes and messages. In such circumstances, the MISO team works with the IO element to produce themes and messages that can be used by the unit to support operations.

(U) Developing Themes

- Normally, themes are provided by higher headquarters. Themes typically support approved command lines of operation, MISO objectives and supporting objectives, and the commander’s communication synchronization guidance.
- Creation of new themes should be undertaken only if existing themes do not meet the needs of the situation.
- A theme can be conceptualized as an argument. The target foreign audience is informed of the desired behavior and told why it will benefit them or improve their overall condition. The theme represents the benefit or improvement.
- There are two broad types of themes:
 - Themes to Stress. These themes are included in plans to communicate messages to target foreign audiences. Themes to stress are typically found in the commander’s communication synchronization guidance, higher headquarters plans and orders, or MISO themes developed at higher echelons. Themes to stress are approved at the National level.
 - Themes to Avoid. These themes are politically sensitive subjects that members of the military must avoid. They frequently include religious and gender topics. MISO guidance usually includes a list of themes to avoid.

(U) Worksheet

This worksheet is a tool for developing themes and messages. It is based on the premise that different themes are needed for each specific target audience.

This worksheet is a tool for developing themes and messages. It is based on the premise that different themes are needed for each specific target audience.	Theme and Message Worksheet				
	Target Audience	Target Audience Vulnerability	Desired Target Audience Action(s)	Themes	Messages

Figure 6-1. Theme and message worksheet.

- First, divide the populace and threat forces into discrete geographic, demographic, and organizational groups. Then, identify the individual and collective foreign target audiences (TAs). The selected TA should be as specific as possible.

- For each TA, identify the primary vulnerability (this can also be thought of as the main interest or concern). Again, be as specific as possible. Instead of identifying something generic like “security,” refine the TA vulnerability to the exact reason the TA feels insecure.
- Next, identify the desired behavior or action for each TA.
- When possible, select pre-existing themes and tailor, as needed, to fit the situation. Absent any appropriate themes, develop new themes that are appealing to the TA and will induce the desired behavior.
- Craft messages that clearly communicate themes to each desired TA (see the other side of this aid).

NOTE: This methodology can be used for a TA within both the foreign populace and threat forces.

Example Theme and Message Worksheet				
Target Audience	Target Audience Vulnerability	Desired Target Audience Action(s)	Themes	Messages
People in Village X	Security from villagers in Town Y	Halt violent demonstrations	Violence does not solve any problems	TBD

Note: this methodology can be used for TA within both the populace and the enemy forces

Figure 6-2. Example theme and message worksheet.

(U) Themes

Themes that embrace the TA’s values, perceptions, and conditions will have the greatest chance of success, to include the following:

- Threat Forces.
 - Inevitability of defeat.
 - Hardship and privation.
 - Absence from loved ones.
- Local Foreign Population.
 - Security and stability.
 - Reconstruction and economic prosperity.
 - Tribal and cultural values (i.e., Pashtunwali).

- Nationality and history (i.e., Bosnia is a multi-ethnic state).
- Insurgents are criminals.
- Foreign Governments.
 - Commitment and resolve.
 - International security.
 - Cooperation.
- Third-Party Organizations.
 - Security and stability.
 - Solidarity with military forces.
- Themes to Avoid.
 - Religion (i.e., Islam vs Christianity).
 - Gender roles and treatment.
 - Political and social factionalism.

(U) Types of Messages

When possible, message content should address TA vulnerability, such as the following:

- Motives. Look for factors that drive TA behavior. Primary motives include basic life needs such as shelter, security, and food. Secondary motives evolve from social interaction within the family, clan, or tribe; or from membership in political and religious organizations.
- Demographics. Look for TA characteristics such as gender, ethnicity, religion, and age. Not all characteristics are vulnerabilities. Planners must determine which characteristics can be exploited to affect TA behavior.
- Psychographics. Look for TA's cognitive characteristics relevant to the world around them, both near and far. These can be values, beliefs, attitudes, and ideology that will trigger an emotional response.
- Symbols. Any video, audio, or audio-visual object or symbol that bears cultural or contextual significance to the TA.

Once vulnerabilities are identified, messages are crafted that communicate approved themes to the TA and address the TA's vulnerabilities.

(U) Crafting Messages

Messages are created in the context of relevant military, political, or social factors, such as the following:

- Effective messaging is couched in the language of the TA.
- Keep each message succinct. Complex messages pose challenges for senders, translators, and receivers. Limit each message to one sentence.
- Tailor messages for the means and method of delivery and the TA.
- Keep messages to a manageable number: perhaps five per theme or TA.
- Convey a story (i.e., the theme) by arranging the messages from first to last. The sum of the messages should support the commander's narrative and tell the story (or theme).
- Put the bottom line up front and summarize at the end. The first message should contain the most important thought. The last message should restate the first message.

(FOUO) Example Messages

Theme: It is inevitable that the insurgents will be defeated.

- While your leaders sleep safe in their warm beds, you are left to suffer in the cold.
- Your mothers will mourn the deaths of their sons and your children will be orphans when you meet the bloody death that awaits you.
- Lay down your weapons and return home to the families who need you.

Theme: The Army is honorable and capable.

- The Army is the guardian of the people.
- The Soldiers fight like bold lions for the freedom of the nation.
- The enemy comes with foreigners in the night to murder and rob its fellow tribesmen.
- Help the Army defeat its enemies and provide information about terrorists weapons, people, and activities.

Theme: The insurgents are responsible for civilian deaths.

- The United States and its allies do everything possible to avoid civilian deaths.
- The insurgents hide among the populace.
- It is well known that the terrorists place women and children in harm's way when it suits the terrorists' purposes.

(U) Conduit Selection

Messaging is passed to TAs through conduits (e.g., broadcast, print, electronic, face-to-face). Each conduit has its own unique characteristics.

When selecting conduits, consider the following:

- Determine which conduit is best for engaging each TA. Certain conduits may be better for certain types of TAs (e.g., individuals or groups) — is the TA receptive to the chosen conduit?
- Determine TA accessibility — can the selected conduit reach the TA?
- Consider the employment of host nation media outlets if these are advantageously positioned to reach the TA.
- Consider that the conduit itself may impact message format and content.
- Consider that certain assets and conduits are subject to constraints imposed by national and theater policy, as well as political and cultural considerations.

Chapter 7

Information Operations Working Group

This chapter describes what preparations and sections are needed to plan and conduct an information operations working group (IOWG).

This chapter is based on tactics, techniques, and procedures used in pre-deployment training at 1st Information Operations Command (Land) to augment doctrine.

(U) IOWG

A working group is a temporary grouping of predetermined staff representatives who meet to coordinate and provide recommendations for a particular purpose or function. Some working groups may be thought of as ad hoc cells. Others are forums used to synchronize contributions of multiple cells to a process. Depending on the situation or echelon, the IOWG can be either type of working group.

(U) Role of the IOWG

The IOWG brings together representatives of those staff elements concerned with synchronizing and de-conflicting the generation of effects within the information environment (IE) through the combined, methodical employment of information-related capabilities (IRCs) in information support operations (ISO). It is the most important meeting held by the unit's information operations (IO) officer or lead. Unit standard operating procedures should address the following for the working group:

- Purpose. The purpose of the IOWG is to synchronize and de-conflict the generation of effects within the IE through the combined, methodical employment of IRC's ISO operational objectives.
- Frequency. The frequency of IOWGs depends on the situation and echelon. The working group may gather daily, weekly, or monthly. Corps and division headquarters may have daily (combat operations) or weekly (stability operations) IOWGs. Battalion and brigade headquarters normally have fewer working groups than higher echelons.
- Composition (chair and attendees). Participation in the IOWG is determined by the IO element and is a mix of staff element representatives and subject-matter experts (SMEs).
- Inputs and outputs. Attendees must know what information, products, and formats they are required to produce and use.

- Agenda. The formality of an IOWG varies by echelon. However, for purposes of organization and focus, even the simplest IOWG should have an agenda.

(U) Composition

The composition of the IOWG is tailored to support current and future operations. The agenda for each IOWG varies in terms of content, but the format remains consistent. Representatives from every staff do not need to attend every IOWG, nor do they participate throughout all portions of the IOWG. Participants are selected because they are IRC managers, staff principals, special staff, and/or external support SMEs. Typical representation and participation can include the following:

- Staff IO Officer. Subordinate unit IO officer(s) and/or designated representative(s).
- Staff IRC Managers.
 - Operations security officer.
 - Military information support operations officer.
 - Electronic warfare officer.
 - Military deception officer.
- External Support.
 - Army IO unit support team leader.
 - Army cyberspace operations support team leader.
 - Combat camera officer/team leader.
- Other Staff Principals.
 - G-2/S-2 and/or designated representative.
 - * Counterintelligence officer and/or designated representative.
 - * Offensive cyberspace operations SME.
 - * Electronic support SME.
 - G-3/S-3 and/or designated representative.
 - * Fire support/targeting officer and/or designated representative.
 - * Special technical officer and/or designated representative.

- * Special operations liaison officer and/or designated representative.
- * Physical security SME.
- G-5/S-5 and/or designated representative.
- G-6/S-6 and/or designated representative.
 - * Defensive cyberspace operations SME.
 - * Electromagnetic spectrum operations SME.
 - * Information assurance SME.
- G-9/S-9 and/or designated representative.
- Special Staff.
 - Public affairs officer and/or designated representative.
 - Chaplain and/or designated representative.
 - Judge advocate general officer and/or designated representative.
 - Cultural adviser.
 - Knowledge management SME.

(U) Duties and Responsibilities

- IO Element.
 - Chair and facilitate working group.
 - Establish and enforce agenda.
 - Encourage active participation.
- IRC Managers.
 - Serve as SME for the staff function or unit.
 - Provide input on asset status.
 - Provide input on current and future tasks and activities.
- G-2/S-2.
 - Provide intelligence relevant to IO.
 - Answer working group requests for information (RFIs).

- Propose and de-conflict IE effects to counter threat activities directed against friendly intelligence, surveillance, and reconnaissance activities.
- G-3/S-3.
 - Provide input on current and future operations.
 - Propose and de-conflict IE effects on ISO's current and future operations.
- G-5/S-5.
 - Provide input on plans.
 - Propose and de-conflict IE effects on ISO's planned operations.
- G-6/S-6.
 - Provide input on the status of the network.
 - Address the deputy commanding officer (DCO), information assurance (IA), and electromagnetic spectrum operations (EMSO) issues and RFIs.
 - Propose and de-conflict IE effects on ISO's network operations, DCO, IA, and EMSO activities.
- G-9/S-9.
 - Provide input on current and future civil affairs activities.
 - Propose and de-conflict IE effects on ISO's civil affairs activities.
 - Address civil affairs RFIs and requests for support.
- Subordinate Unit IO Elements/Liaison Officers.
 - Serve as SME for the unit.
 - Provide input on current and future missions, priorities, and tasks.
- Recorder. Record, write, and disseminate minutes of working group.
- Other Participants.
 - Serve as SME for the staff function or area of expertise.
 - Actively participate in the working group.
 - Propose and de-conflict IE effects on ISO operations.

(U) Preparation

Preparation is the key to a successful IOWG and is a collective effort from the IO element. For example, someone sets and prepares the agenda. Another person notifies participants and ensures each is prepared to provide meaningful input to the working group. Yet another person prepares the IOWG presentation.

Preparation tasks include the following:

- Set agenda.
- Notify participants by performing the following:
 - Verify time and place of IOWG.
 - Identify additional participants.
- Review status of due-outs — contact those participants with due-outs.
- Coordinate with participants who have formal input.
- Publish a read-ahead packet, to include the following:
 - If possible, provide IOWG materials to participants prior to the meeting.
 - Ensure participants provide input to IOWG presentation prior to the meeting.
- Assign a recorder to take minutes for the working group.

(U) Working Group Basics

- Certain basics of meeting management can increase IOWG effectiveness.
- Establish consistent meeting times and places.
- Keep meetings short (one hour is a good rule of thumb).
- Have an agenda and follow it.
- Tailor working group membership to those people who are truly needed.
- Encourage participation — working groups are not one-way conversations.
- Complete detailed work and coordinate actions before the IOWG meets.

- Discuss only actions and issues that are relevant to the working group.
- Identify and work critical issues (leave side-bar issues after the working group).
- Follow through on actions and due-outs. Record and track the results of the working group. Publish minutes.
- Insist on timely delivery of due-outs and products.
- Invite subordinate and higher command representatives.
- Give feedback to working group members.

(U) Agenda

IOWG agendas vary by mission, situation, and echelon. A good basic template for an IOWG agenda includes the following:

- Roll call.
- Intelligence update.
- Operations update.
- Review of due-outs.
- Due-outs from previous IOWG.
- Assessment update.
- Discussion and/or issues.
- Conclusion.

IOWGs are often organized along the lines of either a targeting or operations meeting. Regardless of agenda, the purpose of an IOWG remains the same — to synchronize and de-conflict the generation of effects within the IE through the combined, methodical employment of IRCs of ISO operational objectives.

(U) Due-Outs

Due-outs address unanswered questions or issues from the previous IOWG. Previous due-outs not answered during the IOWG should be carried over for resolution to the next IOWG. Typically, a due-out identifies the issue or question requiring resolution, and the person or element responsible for answering the due-out.

(U) Intelligence Update

The purpose of the intelligence update is to answer current IO intelligence requirements.

- Intelligence updates for IO should not be a regurgitation of other “conventional” intelligence updates. The focus should be on threat activities that are known, or perceived, or projected to occur within the IE and the impact those activities will have on friendly forces.
- One way to structure the intelligence update is to capture significant events in the IE and organize the events by IO staff intelligence requirements.

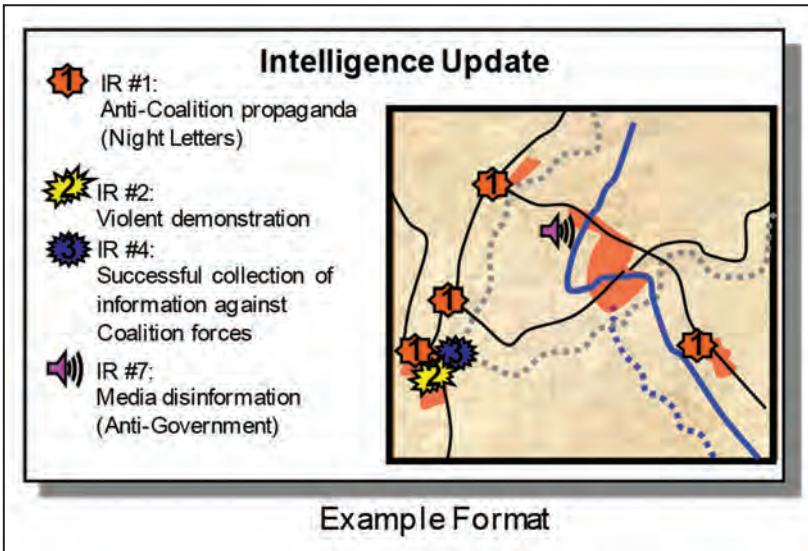


Figure 7-1. Example format of an intelligence update.

(U) Operations Update

The purpose of the operations update is to synchronize and de-conflict the generation of effects within the IE, expressed in terms of IRC tasks and targets supporting current and future operations. The focus is on gaining or maintaining an information advantage within the IE that translates into a realizable and predictable advantage in the overall operational environment.

One way to structure the operations update is to use graphics that show time, location, and purpose for key IO tasks for each major operation.

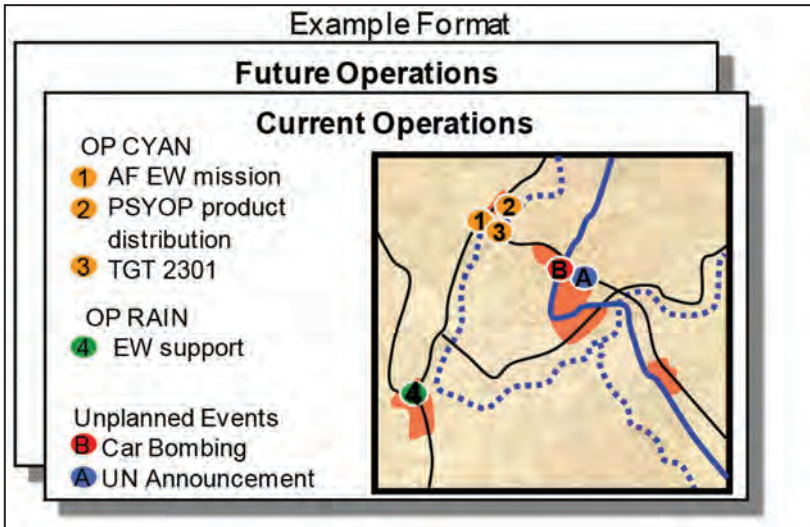


Figure 7-2. Example format of current and future operations.

(U) Discussion/Issues

The purpose of discussing issues or special topics is to support IO decisionmaking and to synchronize and de-conflict the current/future generation of IE effects through the combined, methodical employment of IRCs in ISO operations.

The IO officer selects discussion topics. Working group participants have the opportunity (and responsibility) to discuss the topics from the perspective of their staff function or area of expertise.

This discussion can be facilitated or focused by the use of an operations calendar containing critical events and planned operations.

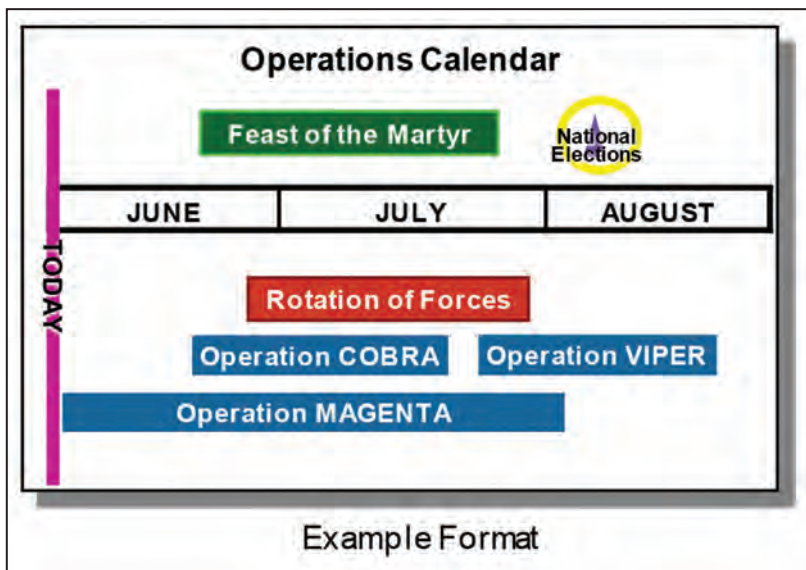


Figure 7-3. Example format of an operations calendar.

(U) Assessment Update

The purpose of the assessment update is to assess the impact and effectiveness of the current generation of IE effects as part of the broadly planned information operations concept of support.

- The focus is on analyzing and presenting information and intelligence from unit reports, as well as input from the IOWG members.
- The example shown in Figure 7-4 is a way assessment can be graphically depicted — each operational area has a pie chart that represents the status of the current IO objectives (in this example there are five IO objectives).

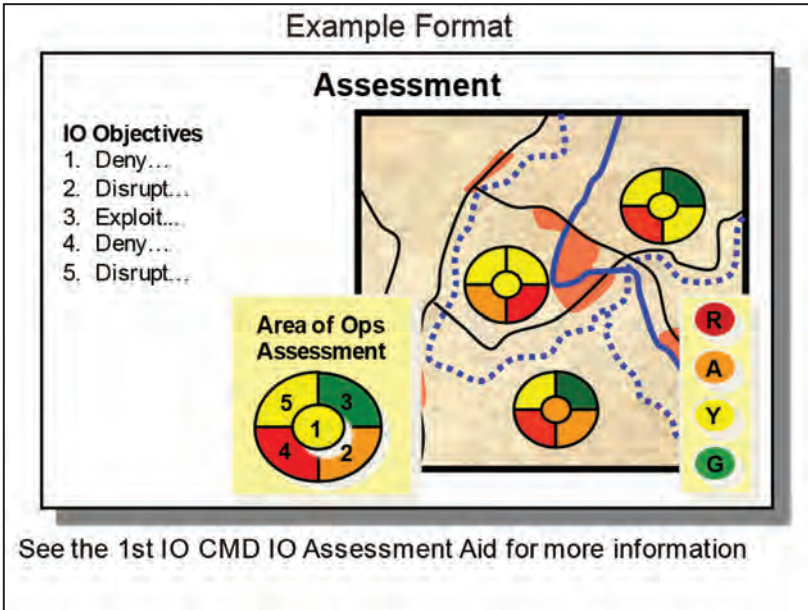


Figure 7-4. Example format of an assessment graph.

(U) Review of Due-Outs

The purpose of reviewing due-outs is to ensure the working group participants understand and acknowledge their due-outs and responsibilities for the next meeting. Prior to final questions and comments, the IO officer reviews new due-outs identified during the working group as well as any open due-outs from the previous working groups. Each due-out should identify the issue or question requiring resolution, and the person or element responsible for answering the due-out.

(U) Conclusion

The IO officer briefly discusses what the meeting accomplished and what working group objectives were met. If necessary, sidebar conversations, meetings, and other sub-working groups are identified and scheduled.

Chapter 8

Tactical Operations Security

This chapter describes how to plan operations security (OPSEC) as part of an information operation in support of tactical operations.

This chapter is designed to augment doctrine based on 1st Information Operations Command (Land) tactics, techniques, and procedures for pre-deployment training.

(U) OPSEC Terms

Essential Secrecy. The condition achieved by the denial of critical information to threat forces. Essential secrecy depends on the combination of two approaches to protection: (1) Security programs to protect classified information, and (2) OPSEC to deny threat forces critical information, which is often unclassified:

$$\text{Essential Secrecy} = \text{Security Programs} + \text{OPSEC}$$

Critical Information. Specific facts about friendly intentions, capabilities, and activities vitally needed by threat forces to plan and act effectively to guarantee failure or unacceptable consequence for friendly mission accomplishment.

OPSEC Indicator. Detectable actions and open-source information that can be interpreted or pieced together by threat forces to derive critical information.

OPSEC Vulnerability. A condition in which friendly actions provide OPSEC indicators obtained and accurately evaluated by threat forces in time to provide a basis for effective threat decisionmaking.

(U) OPSEC and Military Decisionmaking Process

OPSEC should be included in every plan, operation, and activity. The OPSEC process is a way to systematically identify, analyze, and protect information. The goal of OPSEC, in conjunction with unit security programs, is to achieve essential secrecy. The OPSEC process should be integrated into the military decisionmaking process.

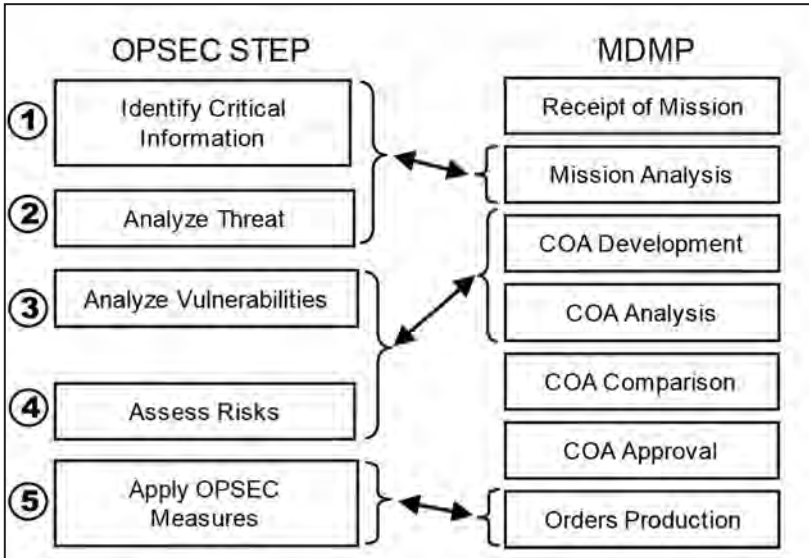


Figure 8-1. OPSEC steps integrated into the military decisionmaking process.

(FOUO) Identify Critical Information

Determine what information must be protected, and create the critical information list (CIL):

- Identify what information is critical to friendly operations. Sources of critical information include: higher headquarters plans, the operations order, commander’s guidance, and current unit CIL.
- Focus CIL on friendly force:
 - Intentions (time and place of units and operations).
 - Capabilities and vulnerabilities (strength, technologies, tactics).
- CIL is different for every operation, do not use a “cookie-cutter” approach.
- Use an OPSEC working group (OWG) to take advantage of subject-matter experts (i.e., aviation, communications and computer systems, etc.).
- Identify the length of time each CIL item must be protected (not all information needs protection for the duration of the operation).
- Prioritize CIL and keep to a manageable number (perhaps five).

CIL	Vul	Indicators	Enemy Collection	Risk Level	OPSEC Measure	Residual Risk	Assess
Location of Unit Elements	Assault Force Insertion	Rotary Wing Movement	Sympathetic Populace	E	False Insertions	M	No enemy contact on movement
		Ground Movement	Spotters	H	Recon element placed on route	L	Enemy surprised on objective

Useful format for determining risk to CIL

OPSEC Worksheets

CIL	Enemy Collection Capabilities	Vulnerable Indicators	SOP or Current OPSEC Measures	Additional OPSEC Measures	OPSEC Tasks
Task Organization	Spotters on FOB and MSRs	Vehicle Markings	Cover vehicle markings	Remove unit markings	1st Bn 2nd Bn 3rd Bn
		Command vehicles	None	No unsecured comms	BDE HQ

Useful format for planning OPSEC tasks

Figure 8-2. OPSEC worksheets.

(FOUO) Critical Information List (CIL)

CIL should be written in the form of a statement. Generic examples include the following:

- Current and future locations of unit elements.
- Intelligence, surveillance, and reconnaissance capabilities and limitations.
- Unit movement methods and routes.

(U) OPSEC Working Group (OWG)

- The OWG is a group of subject matter experts who perform the following:
 - Determine critical information by producing a CIL.
 - Identify OPSEC vulnerabilities.
 - Coordinate and synchronize OPSEC measures and tasks.
 - Assess effectiveness of OPSEC tasks.
- Typical membership includes the OPSEC officer, information operations element personnel, intelligence analyst, counterintelligence personnel, force protection officer, communications and aviation representatives, and subordinate unit liaison officers.
- The OWG should conduct periodic assessments of CIL, threat collection capabilities, OPSEC vulnerabilities, and OPSEC measures.
- OWG principles include the following:
 - Stay focused on OPSEC.
 - Meet on a regular basis.
 - Quickly respond to OPSEC-related issues.
 - Must produce something.

(FOUO) Analyze Threat

- Identify the threat to the CIL.

Threat to CIL = Enemy Information Needs + Collection Capabilities

- Identify enemy information needs and collection capabilities.
 - Information needs. What does the enemy already know?
 - Collection capabilities: Human intelligence, signal intelligence, imagery intelligence, and open-source intelligence (Keep in mind that 90 percent of enemy information needs are met from open-source intelligence).

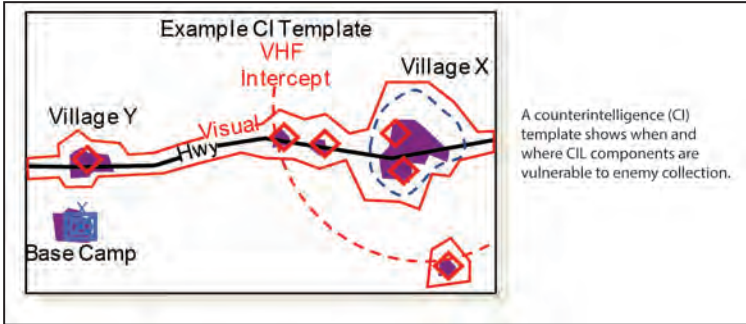


Figure 8-3. A counterintelligence template showing when and where the CIL are vulnerable to enemy collection.

(FOUO) Analyze Vulnerabilities

Identify each component of the CIL vulnerable to enemy intelligence collection.

$$\text{OPSEC Vulnerability} = \text{OPSEC Indicator} + \text{Enemy Collection Capabilities}$$

- OPSEC vulnerabilities are detectable indicators of the CIL.
- An OPSEC indicator becomes an OPSEC vulnerability if it can be observed, analyzed, and acted upon by the threat.
- To determine OPSEC vulnerabilities:
 - Identify OPSEC indicators. Determine what detectable actions and open-source information can be interpreted or pieced together by the threat to derive CIL.
 - Compare OPSEC indicators to enemy collection capabilities. Determine which indicators can be observed, analyzed, and acted upon by the threat.

(FOUO) Assess Risk

Develop measures to protect OPSEC vulnerabilities.

- Conduct risk assessment for each vulnerability.
- Select one or more OPSEC measures for each vulnerability.
- Three types of OPSEC measures:
 - Action controls that change unit procedures, activity, and actions (i.e., randomized routine activities, avoidance of repetitive tactics and procedures).

- Countermeasures that disrupt enemy information gathering and targeting (jamming as part of electronic warfare, physical attack, camouflage and concealment).
- Counter analysis that provides false indicators to deceive the threat (decoys, deception in support of OPSEC).
- Decide which OPSEC measures to recommend to the commander for implementation, and check that OPSEC measures do not create new vulnerabilities.

Balance OPSEC measures with operational effectiveness (i.e., risk versus unit resources).

(U) Example Risk Assessment

Risk assessment can be used to select OPSEC measures that lower unit vulnerabilities to an acceptable level. See FM 3-100.12, *Risk Management*, for information.

Vulnerability	Vulnerability Rating	Threat Rating	Overall Risk	Accepted Risk	OPSEC Measure	Residual Risk
Base Camp Departure	E	E	E	NO	Move at Night	H
				YES	Indirect Route	M

- This chart shows an initial unacceptable risk level (E).
- Conducting the movement at night is determined to bring the risk level down to H. This is still an unacceptable risk. Look for an additional OPSEC measure to lower the residual risk to ≤ M.
- Taking an indirect route, added with the initial OPSEC measure of moving at night, is determined to bring the level to M. The commander has determined this to be an acceptable risk.

(FOUO) Apply OPSEC Measures and Develop Tasks to Units and Staff

- Rewrite approved OPSEC measures as tasks.
- Assign responsibility and coordinate OPSEC tasks with units and staff.
- Coordinate OPSEC measures with military deception, public affairs, and combat camera to prevent compromise of CIL.
- Integrate OPSEC tasks with information operations planning and synchronization.

- Include OPSEC tasks in the operations plan/order.
- Adjust OPSEC measures based on threat reaction to the implemented OPSEC measures.
- Coordinate monitoring of OPSEC measures through G-2.

(U) OPSEC Assessment

Conduct OPSEC assessments before and during the mission to validate the following:

- Is CIL current?
- Does CIL match the threat's current information needs?
- Have threat intent or capabilities changed?
- Have additional vulnerabilities or indicators been created?
- Are unit members knowledgeable on CIL and threat collection methods?
- Are effective OPSEC measures in place, or planned, to protect CIL?
- Are subordinate commanders employing OPSEC?

Monitor operations for CIL compromises. In such cases, provide options and recommendations to the commander.

(U) OPSEC Standing Operating Procedure

An OPSEC standing operating procedure (SOP) is critical to ingraining OPSEC into unit operations. Keep the SOP short and direct. As a minimum, include the following:

- Standing CIL and standing OPSEC measures.
- Composition and responsibilities of the OWG.
- OPSEC assessment procedures.

Chapter 9

Tactical Deception

This chapter describes how to plan a deception operation in support of tactical ground operations.

This planning aid is designed to augment doctrine, based on 1st Information Operations Command (Land) tactics, techniques, and procedures in pre-deployment training.

(U) Deception Terms

Deception Objective. Purpose of the deception operation in terms of the action or inaction that is desired from the enemy.

Deception Target. The threat decisionmaker with the authority to make the decision that will achieve the deception objective.

Desired Perceptions. What the deception target must believe to make the decision that will achieve the deception objective.

Story. The scenario that outlines friendly actions that will be portrayed to the threat.

Means. The methods, resources, and techniques used to act out the deception story. Deception means will vary by unit, echelon, and mission.

Events. Activities conducted by the deception means at a specific time and location to convey the deception story. These activities are “seen” by the enemy intelligence system.

Feedback. Indications of how the target is responding to the deception.

(U) Deception Planning

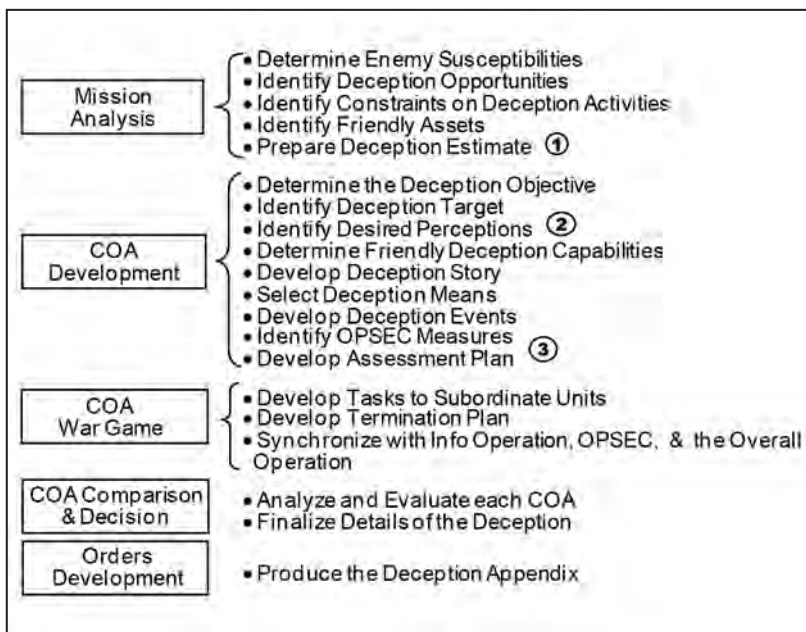


Figure 9-1. Planning a deception operation in support of tactical ground operations.

Deception Estimate Format

1. Mission	<ul style="list-style-type: none"> • Restated mission of the command • Deception objective – Identify the purpose of the deception
2. Situation & Course of Action	<ul style="list-style-type: none"> • Summarize the situation in terms of: characteristics of the AO, enemy situation, friendly situation, assumptions • Identify friendly deception COA
3. Analysis of Deception COAs	For each deception COA list: the target vulnerability analysis, desired perceptions, deception story, means, events, risk analysis, & probability of success assessment
4. Comparison of Deception COAs	Compare deception COAs in terms of: costs and benefits, operational risks, comparative strengths, weaknesses, and probabilities of success
5. Recommendation	Recommend a deception COA

Note: Estimates can be a text document or a graphic presentation.

Figure 9-2. Example deception estimate.

Desired Perceptions. Desired perceptions are those thoughts the target must process in order to believe the planned deception story and take the desired action. The formation of the target's perceptions is largely based on the means and events used to portray the deception story.

Means Development. Considerations for selecting deception means include the following:

- What collection system/mechanisms does the target use?
- How much credibility does the target place on information from each conduit?
- What kind of information can be conveyed through each means?
- When is each means available to transmit information?
- How long will it take for the information to reach the target?

Events. The deception story is portrayed to the target through deception events conducted by friendly forces. These are pieces of a puzzle that the target assembles over time. The puzzle itself is the deception story, the pieces are the deceptive events seen by the target via the means. Events must be observed and accepted as reality by the target. There are two types of deception events: those necessary for the formation of desired perceptions (required events); and supporting events that complement or reinforce the desired perceptions.

Assessment Plan. There are two primary forms of feedback in deception operations:

- **Indicator Feedback.**
 - Information that indicates whether and how the deception story is reaching the deception target. Useful for the timing and sequencing of executions.
 - Answers the question: Is the target receiving the deception story as planned?
- **Perception Feedback.**
 - Information that shows whether the target is forming the desired perceptions and is acting in accordance with the deception objective.
 - Answers the question: Is the target acting in accordance with the deception objective?

At the tactical level, the pace of operations and limited number of collection assets may reduce the practicality and utility of feedback. For this reason,

at the lowest levels of command, tactical deception operations must not depend on feedback for successful execution.

(U) Deception Techniques

Tactical deceptions often contain one or more of the following techniques:

- **Feint.** A limited operation to deceive the enemy of the location or time of the decisive operation. Feints usually occur before or during the main operation. Multiple feints may be needed to portray the deception story. The objective of a feint is to cause the enemy to misemploy forces.
- **Demonstration.** A show of force to deceive the enemy as to the location or time of the decisive operation. It is similar to a feint, except no contact is made with the enemy. The objective is to delude the enemy into an unfavorable course of action. Useful when time and distance factors make the lack of contact realistic.
- **Ruse.** Deliberate exposure of false information to enemy collection means.
- **Display.** A static display of an activity, force, or equipment intended to deceive enemy observation. Displays project the appearance of objects that do not exist or appear to be something else. Observables include the use of heat, smoke, electronic emissions, false tracks, or fake command posts.

(U) Deception Tactics

Ambiguity Increasing. Increases decisionmaker uncertainty about key information needed to make decisions. It can be used to delay or reduce the quality of a decision.

- Present conflicting elements of information.
- Overload enemy intelligence collection and analytical capabilities.
- Confuse enemy expectations about friendly force size, activity, location, unit, time, equipment, intent, or mission.

Ambiguity Decreasing. Provides the decisionmaker with the illusion of reduced uncertainty and risk. It can be used to elicit specific behavior that can be exploited by friendly forces, and to provide cover for friendly actions.

- Reinforce the threat's preconceived beliefs.
- Draw threat attention from one set of activities to another.
- Create the illusion of strength where weakness exists.

- Create the illusion of weakness where strength exists.
- Accustom the threat to patterns of activity that are exploitable at a later time.

(U) Planning Matrices

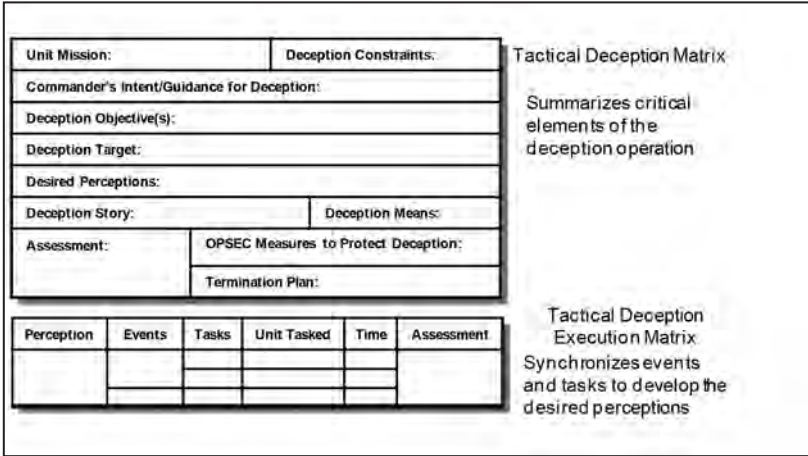


Figure 9-3. Example tactical deception planning matrix.

(U) Deception and Psychological Operations

At the tactical level, military information support operations (MISO) is a primary deception capability. Tactical MISO units may conduct tactical deception using sonic deception (i.e., loudspeakers) for force protection and in support of direct action missions.

(U) Deception and Combat Operations

In support of combat operations, deception can preserve friendly forces and equipment from destruction, gain time, or minimize an enemy's advantage. A deception is most effective if the friendly force has more courses of action available than the enemy has forces to cover in strength.

- **Purpose.** Create an operational advantage through surprise.
- **Possible Objectives.**
 - Delay or prevent enemy action or counteraction.
 - Cause enemy to misdirect reconnaissance, intelligence, surveillance, and target acquisition.
 - Cause the enemy to employ forces in ways that make the enemy vulnerable.

- Cause the enemy to reveal strengths, dispositions, and intentions.
- Cause the enemy to waste combat power with inappropriate or delayed actions.
- **Target.** Threat commander.

(U) Deception in Support of Stability Operations

Deception may improve force protection, mask intentions, and deter threat actions.

- **Purpose.** Degrade threat attempts to disrupt peace.
- **Possible Objectives.**
 - Prevent hostile forces from attacking friendly forces (force protection).
 - Deter factional violence.
- **Target.** Violent faction leaders.
- **Considerations.**
 - Political objectives may prevent the use of deception.
 - Participation of allied forces may restrict the utility and use of deception.
 - Exploitable conduits may be small and are likely to be non-technical.
 - Non-lethal environment may restrict deception means and methods.

(U) Deceptions in Support of OPSEC (DISO)

A DISO increases the number of indicators that the threat can observe to derive an incorrect conclusion. It hides real indicators while showing fake indicators. Observables are presented to distract threat intelligence collection away from, or provide cover for, real friendly operations and activities.

- **Purpose.** Degrade threat intelligence collection capabilities.
- **Objective.** Induce error into threat intelligence collection and analysis.
- **Targets.** Threat intelligence collection and analysis systems.

(U) Deception in Support of Counterinsurgency

During counterinsurgency missions, selection of deception targets may not be possible. In lieu of a known target, planners can use profiles of cell leaders. Counter-deception is important, as insurgent and guerrilla warfare theory emphasizes the use of deception to accomplish goals.

- **Purpose.** Degrade threat recruiting efforts.
- **Possible Objective.** Cause threat forces to be seen by friendly collection assets.
- **Target.** Insurgent (cell) leaders.

Chapter 10

Combat Camera

This chapter describes how to employ combat camera (COMCAM) teams as an information operations capability in support of tactical ground operations.

This planning aid is designed to augment doctrine, based on 1st Information Operations Command (Land) tactics, techniques, and procedures in pre-deployment training.

(U) Combat Camera Terms

Visual Information

- Use of one or more of the various visual media with or without sound.
- Generally, visual information includes still photography, motion picture photography, video or audio recording, graphic arts, visual aids, models, displays, visual presentation services, and the support processes.

Visual Information Documentation (VIDOC)

- Motion media, still photography, and audio recording of technical and nontechnical events while they occur, usually not controlled by the recording crew.
- Visual information documentation encompasses combat camera, operation documentation, and technical documentation.

Joint Combat Camera Center (JCCC)

- The Department of Defense (DOD) central collection point for all still and motion imagery.
- The JCCC electronically processes and edits imagery acquired by DOD photographers, primarily operating in Joint and service COMCAM teams deployed in wartime, contingency and humanitarian operations, Joint exercises, and other operations or events involving U.S. military forces.

(U) COMCAM Principles

COMCAM operations provide commanders with classified and unclassified still and motion VIDOC support. Each service's COMCAM organization provides service-unique VIDOC capabilities.

Army. Army COMCAM units provide still and video acquisition of all operations to include land, static airborne, and air assault operations.

Army COMCAM units are trained and equipped to operate under all weather and lighting conditions, with both conventional and special operations units. These units maintain airborne-qualified Soldiers and conduct other advanced tactical training to include air assault, combat lifesaver, combative, and advanced marksmanship techniques. The 55th Signal Company (Combat Camera) is the only active duty combat camera company in the U.S. Army.

Air Force. The primary role of Air Force COMCAM units is the VIDOC of Air Force combat operations. The Air Force COMCAM units' secondary role is the centralized collection, management, and distribution of imagery (including weapons system video imagery). These units are fully qualified and equipped for day and night operations. COMCAM units also possess fully qualified aircrew members for aerial documentation.

(U) Service COMCAM Capabilities

COMCAM operations provide commanders with classified and unclassified still and motion VIDOC support. Each service's COMCAM has unique capabilities.

Marine Corps. COMCAM units are organized to support imagery requirements at all levels within the Marine Air-Ground Task Force (MAGTF). Operational COMCAM assets are organic to all Marine divisions, Marine aircraft wings, Marine logistics groups, and all Marine expeditionary units. U.S. Marine Corps operational COMCAM units provide the MAGTF commander direct imagery tactical printing support in the form of photography, video-graphic, graphic arts, and lithography. MAGTF COMCAM teams deploy with man-pack systems capable of all-weather, day and night digital acquisition. The teams use organic U.S. Marine Corps communications systems to disseminate imagery and imagery products both horizontally and vertically throughout the MAGTF.

Navy. COMCAM units include aircrew- and diver-qualified personnel to provide specialized support to day and night operations, all-weather aerial (fixed- and rotary-wing) and maritime operations, underwater operations (fleet combat camera, Atlantic only), and battlespace imagery acquisition and transmission capabilities.

Army. COMCAM units provide still and video acquisition of operations to include land, static airborne, and air assault operations. Unit personnel are trained and equipped to operate under all weather and lighting conditions with both conventional and special operations units. The units maintain airborne-qualified Soldiers and conduct other advanced tactical training to include air assault, combat lifesaver, combative, and advanced marksmanship techniques. The 55th Signal Company (Combat Camera) is the U.S. Army's only active duty combat camera company.

Air Force. The primary role of COMCAM units in the U.S. Air Force is the VIDOC of Air Force combat operations. The units' secondary role is the centralized collection, management, and distribution of imagery (including weapons system video imagery). Unit personnel are fully qualified and equipped for day and night operations. COMCAM units also possess fully qualified aircrew members for aerial documentation.

(U) COMCAM Operations

COMCAM supports the commander by acquiring, processing, and distributing classified and unclassified still and motion imagery, collected during ongoing operations. COMCAM can be employed wherever the mission dictates and is often employed to provide the following:

- **Gather Intelligence.** Provide imagery of potential targets or target areas, and support battle-damage assessments.
- **Support Planning Efforts.** Validate assumptions by providing accurate images of a situation.
- **Provide Imagery to Public Affairs (PA).** Provide graphics, photography, video products, and print media to enhance the effectiveness of PA products.
- **Document Interrogations and Autopsies.** Provide evidence of proper techniques and procedures.
- **Support Landing Zone Studies.** Imagery can help determine the diameter of the area and the terrain's grade.
- **Provide Historical Documentation.** Provide evidence of events for future use (i.e., Red Cross investigation) and preserve the accuracy of historical military events (i.e., Normandy Invasion, release of prisoners from Nazi concentration camps).

(U) Maximizing COMCAM Support

- COMCAM is an operational asset assigned to the J-3/G-3/S-3. Identify a COMCAM representative within the J-3/G-3/S-3 to plan for the employment of COMCAM.
- Plan to employ COMCAM during the initial phases of an operation to ensure comprehensive mission documentation.
- Ensure COMCAM:
 - Has full mission access, as is reasonably and tactically feasible, during each phase of the operation.
 - Is available for coverage before, during, and after operations.

- Tasks include clearly defined requirements and priorities. Include a purpose for each task to take advantage of COMCAM personnel initiative.
- Imagery is reviewed by PA and OPSEC prior to release outside of the organization.
- Personnel provide imagery to the JCCC for immediate distribution in order to support strategic and operational objectives.

(U) Joint Combat Camera Center

Upon approval by the supported commander, COMCAM teams are required to forward imagery to the JCCC. The JCCC consolidates COMCAM imagery for global distribution.

JCCC customers include the Office of the Secretary of Defense, the Joint Staff, defense agencies, Department of State, Department of Homeland Security, combatant commands, and military and government agencies. Distribution of imagery is accomplished online, via the Defense Imagery Server, managed by the JCCC. It provides still and motion imagery to a worldwide customer base of registered users.

The JCCC is not responsible for clearing imagery for public release. This function is the responsibility of the on-scene commander. The JCCC can receive cleared and uncleared imagery classified up to the SECRET level via electronic means on the SIPRNET. Unclassified imagery that is not cleared for public release should be forwarded to the JCCC with a classification of “For Official Use Only” until cleared by the appropriate PA authority.

(U) Imagery Review Process

COMCAM imagery must be reviewed by appropriate unit staff members prior to release. The supported commander is the release authority for all collected COMCAM images before the images are transmitted out of theater. The complete cycle from image acquisition to receipt by the Joint Combat Camera Center must occur within 24 hours for the collected imagery to remain a viable decisionmaking tool for national-level leaders. Composition of the review board should be tailored based on the specific unit design. A typical review board includes the following:

- J-2/G-2/S-2 representative for identification of possible intelligence and exposure of classified information.
- OPSEC officer for identification of possible disclosure of unit critical information.

- Judge advocate representative for identification of possible, or perceived, violations of the Laws of War.
- J-3/G-3/S-3 representative for identification of exposed tactics, techniques, and procedures or any contents of imagery that are not desirable for release.
- Public Affairs representative for public release consideration.

(U) Combat Camera Support to Information Operations

COMCAM support to information operations includes the following:

- **Military Information Support Operations (MISO).** Imagery designed to influence threat forces or foreign target audiences. Planners should have access to JCCC imagery data base for product development.
- **Counterpropaganda.** Imagery that enhances credibility of friendly forces to prevent or counter threat propaganda.
- **Military Deception.** Imagery that reinforces the portrayed story.
- **Civil Military Operations.** Imagery that records civic action projects and programs.
- **Other.** Visual evidence of threat force defeats, misconduct, or war crimes that can support MISO.

When COMCAM is not available, any Soldier with a camera can document an event. Take the opportunity to brief Soldiers on the intent and handling of the imagery.

(U) Examples of Combat Camera Employment

- **Counter Insurgency Operations.** Afghan National Army Commandos, supervised by U.S. Special Forces, conducted its first operation in late 2007. In order to reinforce perceptions of host nation military capability and competence, COMCAM documented commando successes. The imagery was released to national and regional media, and used in MISO products disseminated to the local populace.
- **Combat Operations.** In 2004, the 1st Marine Expeditionary Force assaulted the city of Fallujah to eliminate an established insurgent stronghold. COMCAM provided evidence of threat torture facilities, weapons storage sites, etc., in order to justify U.S. operations to a previously uncooperative population. Additionally, imagery was provided to local, regional, and international media, who then portrayed the operation in a positive light.

<p>SITUATION</p> <p>Friendly Forces. Combat Camera (COMCAM) Team X located at Forward Operating Base Blue.</p> <p>Enemy Forces. See Base Plan and Annex B, Intelligence.</p>
<p>MISSION</p> <p>COMCAM documents coalition forces (CF) and commando operations in search of Objective Black in order to provide evidence of success, reduce negative effects of CF operations on local populace, and prevent effective enemy propaganda.</p>
<p>EXECUTION</p> <p>Phase I: Document pre-mission rehearsals. Priority: Commando training.</p> <p>Phase II: Document actions on the objective. Priorities: Threat use of protected areas; threat atrocities against the local populace; detainee operations; evidence of improvised explosive devices; key leader engagements.</p> <p>Phase III: Document post-mission operations. Priority: Commando after action report.</p> <p>Coordinating Instructions. Imagery will not expose unit tactics, techniques, and procedures and other operations security-related indicators. Review imagery and submit to the Joint Combat Camera Center within 24 hours of completion of mission.</p>
<p>SERVICE SUPPORT</p> <p>COMCAM team deploys with still- and full-motion video night capability, 48 hours of rations and water, and basic combat load of ammunition.</p>
<p>COMMAND AND SIGNAL</p> <ul style="list-style-type: none"> • On-scene commander has imagery approval authority. • The Public Affairs Office has public release authority.

Figure 10-1. (U) Example of a COMCAM tab.

Chapter 11

Media Analysis Within the Information Environment

This chapter describes a quick and useful technique for evaluating the impact of media coverage on military operations.

This chapter is designed to augment doctrine, based on 1st Information Operations Command (Land) tactics, techniques, and procedures during pre-deployment training.

(U) Purpose of Media Analysis

- The media analysis presented in this aid is a tool staffs can use to quickly understand and assess the impact of media reporting on friendly and threat activities in the area of operations (AO). This type of media analysis helps the staff perform the following:
 - Maintain situational awareness on media reporting.
 - Evaluate the impact of media reporting on the mission.
 - Identify threat propaganda.
 - Provide data for assessment.
- Other staff elements also may conduct media analysis to support assigned functional areas, such as the following:
 - The Public Affairs Office (PAO) conducts a media content analysis to assess news coverage.
 - The intelligence staff may collect and analyze media reporting as part of open-source intelligence (OSINT).
- The information operations staff must be prepared to analyze the media for the purpose of monitoring changes in the information environment and to counter threat misinformation and propaganda.

(U) Media Analysis Steps

Other than the PAO's media content analysis, there is no established doctrinal method for analyzing the media. The steps identified in Figure 11-1 have been field-tested and can be modified to fit command and staff needs.

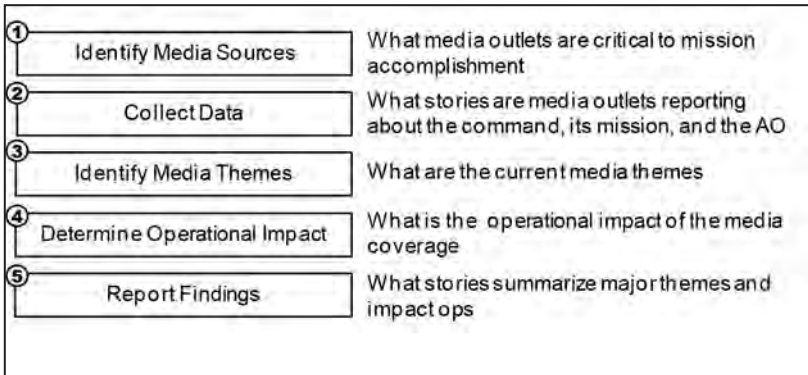


Figure 11-1. Media analysis steps.

(U) Identify Media Sources

Identify media outlets that are critical to mission accomplishment by analyzing the flow of media reporting in the AO and area of interest (AI). Select those media outlets that have local, regional, or international influence. Do not include media outlets that are overtly biased. A good sampling of outlets include the following:

- Local media in the AO. These outlets influence local public opinion.
- Regional media in countries adjacent to the AO. These outlets can influence public and political opinion in the AO and AI. For example, in Afghanistan it is important to monitor the Pakistani press.
- International media are larger outlets associated with countries outside the AO. Typically, these outlets impact U.S. domestic, coalition partner, and worldwide public and political opinion. For example, CBC (Canada); BBC (Britain); Der Spiegel (Germany); and CNN, Washington Post, Los Angeles Times, and the New York Times in the United States.

NOTE: Home/domestic media are a primary focus of the public affairs staff, but are not a consideration for any military information operation.

(U) Collect Data

- Systematically monitor media coverage of the command, its mission, and the AO from the sources identified in Step 1 (see Figure 11-1).
- Useful sources of media reports and stories are:
 - PAO Media Operations Center provides translations of foreign press coverage in addition to major English-language media outlets.
 - OSINT media-monitoring sources contracted by Department of Defense.
 - U.S. Government Open Source Center.
 - The Internet.
- Data collection must be continuous and consistent — usually on a daily basis.
- Several factors can affect collection of data reports, such as the following:
 - English-language media sources are readily available and may skew the collection effort away from local media.
 - Translation of local and regional media may cause a lag time of a day or more.
- A database should be created and maintained to establish a baseline upon which comparisons are made (e.g., media reporting for one month versus another month).

(U) Identify Media Narratives and Themes

Analyze the media coverage collected in Step 2 (see Figure 11-1) to identify current media narratives and themes.

- Pick out primary narratives and themes in the media reports and stories.
- Categorize narratives and themes into groups that either support (positive), run counter (negative) to the command's narrative objectives, or are neutral to threat or friendly forces.
- Identify ad-hoc narratives and themes of interest to the command.
- Associate media sources, narratives, and themes to the command's narrative objectives or lines of operation.

Objective	Theme (+ / -)	Source
Maintain Int'l community support for CF mission	(+) UK supports troop expansion	BBC News CNN
	(-) US missile strikes kill civilians	BBC News AP
Reduce popular support for insurgents	(+) Tribal elders turn in TB to Afghan police	Local AF radio Local AF TV
	(-) TB propaganda about US missile strikes	Dawn (Pakistani newspaper)

Figure 11-2. Associate media sources.

(U) Determine Operational Impact

- Analyze the narratives and themes identified in Step 3 (see Figure 11-1) to determine the impact on friendly and threat operations.
- Categorize media sources, narratives, and themes by echelon (i.e., local, regional, international).
- For each narrative and theme determine the following:
 - Who is the originating source of the narrative or theme?
 - * Threat forces?
 - * Friendly forces?
 - * Third-party organization?
 - * Media embed?
 - Who is the target audience?
 - What is the circulation of the narrative and theme? (Most critical for local media.)

- What are the second and third order effects?
- Is the event affected by extended media coverage (i.e., media bounce)?
- Prioritize narratives and themes within each category based on degree of impact:
 - Determine which negative narratives and themes pose potential problems for on-going and future operations.
 - Determine which positive narratives and themes provide an opportunity for exploitation.

(U) Report Findings

- There is no standard method on how to report media findings.
- The key is to portray media coverage in an easy to understand format that can be quickly scanned to see what narratives and themes are important.
- Use color coding to clearly display the impact of each narrative and theme. For example, Green = positive, Red = negative, Blue = neutral.

NOTE: Add symbols (e.g., +, #, letters, or numbers) so the analysis can be understood if printed in black and white.

- Resist the temptation to fill the boxes with headlines rather than narratives and themes.
- Add in media narratives and themes that reflect threat propaganda.
- Provide an assessment of operational impacts.
- Display a trend analysis to put the current media reporting into a broader context.

(U) Depicting Media Impact

The following format is commonly used in the field:

- List selected narratives and themes by media echelon.
- For each category assess the operational impact.
- Include monthly (last three months) and weekly (perhaps the last 14 or 30 days) trend analysis.

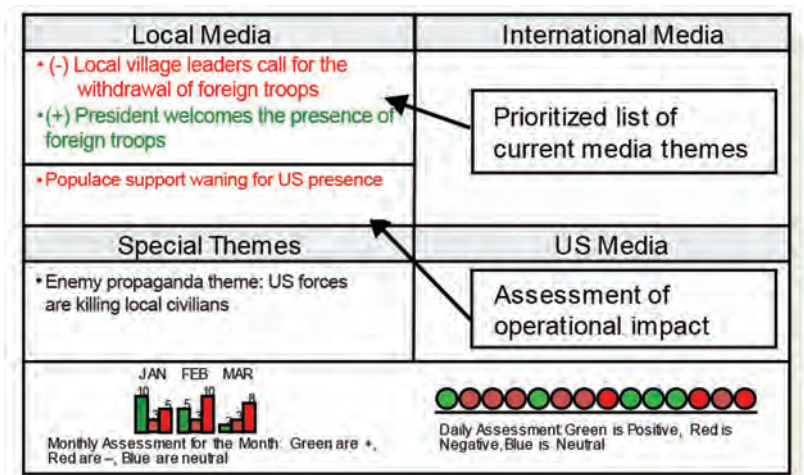


Figure 11-3. Format for media impact.

(U) Consequence Management

- Military operations can trigger either positive or negative coverage by the media. This coverage may be a situation that must be mitigated to prevent or reduce the impact on the unit mission, or exploited as an opportunity to further the command’s objectives. Such a situation is called “media bounce.”
- Media bounce.
 - Refers to the staying power of a story over time.
 - Relatively short time period, particularly if another newsworthy event occurs.
- Monitoring media bounce avoids reacting too quickly to an event that would otherwise lose the media’s attention in a short period of time. Quick reaction often fuels interest and may renew negative reporting, thereby aggravating the situation.

- A consequence management tracker is a simple decisionmaking aid that tracks subsequent media reporting of an event (“bounce”) to determine whether subsequent command action is required. It can provide the following:
 - Help the command and staff to decide what actions, if any, are needed to mitigate a negative event or exploit a positive event.
 - Mitigate ad-hoc reactions to threat propaganda.

(U) Tracking Media “Bounce”

Figure 11-4 conceptually outlines the required components needed for tracking media bounce.

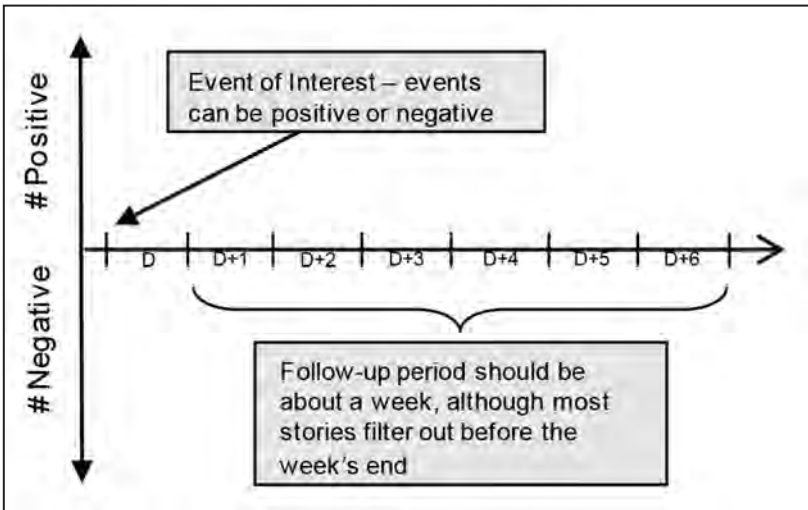


Figure 11-4. Example of components needed to track media bounce.

(U) Consequence Management Example

Figure 11-5 is an example of how media bounce can be used to track negative reporting and shows the lack of media interest four days after the event.

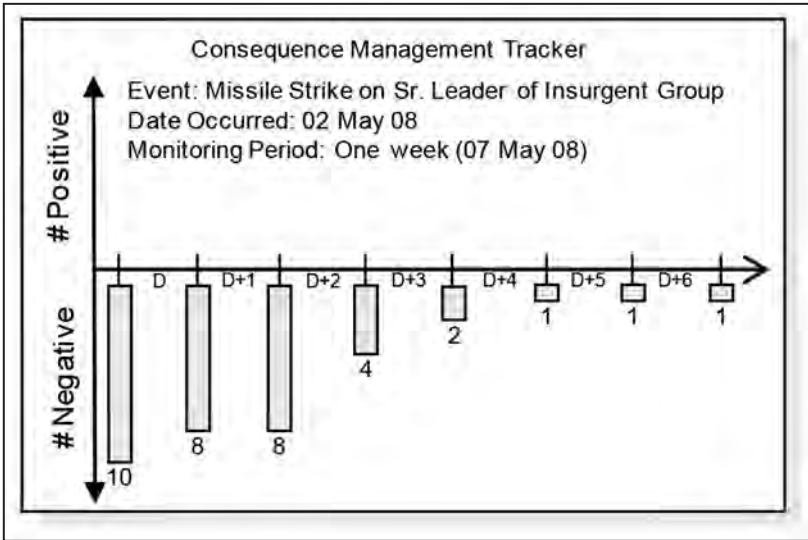


Figure 11-5. Example of tracking negative media coverage.

Chapter 12

Tips for Conducting Face-to-Face Meetings

This chapter is for tactical face-to-face (FtoF) engagements by troops at the squad, platoon, company, battalion, and brigade level when meeting foreign target audiences (TAs).

This planning aid is designed to augment doctrine, based on 1st Information Operations Command (Land) tactics, techniques, and procedures for pre-deployment training.

(U) Preparing for a Face-to-Face Meeting

- **Research.** Learn everything about the foreign TA, such as proper name and title, approximate age, family members, ethnicity, language spoken, and the TA relationship to other leaders, friendly forces, third-party organizations, and the threat.
- **Check Previous Contacts.** Who has had contact with the TA before, when, and what was discussed? Were any promises made? Is the TA truthful, manipulative, and/or trustworthy? What groups/individuals does the TA have ties to?
- **Keep Records.** Take notes (or an aide) during the conversation, refer back to the notes at the end of the FtoF to capture the gist of the conversation. Share the notes with other interested persons.
- **Coordinate.** Coordinate the FtoF to prevent other friendly forces from sending mixed messages to the TA.
- **Set a Time Limit.** Determine how long the meeting should be; stay as close to it as possible, but exploit any available opportunities.
- **Consider Perceptions.** Many factors affect TA perceptions: uniform, long vs. short guns, large vs. small convoy, aircraft in the area, escort, civilians present, number of people attending.
- **Plan for Problems.** Establish code words to maintain control of information flow and security. Typical situations for a code word would include: a desire to end the conversation, potential for violence, increased threat, and possible emergencies.
- **Rehearse.** Practice the discussion with another person through the translator. Solicit comments from anyone who has dealt with the TA before and practice delivery with a translator or other Soldiers.

- **Plan the Rest of the Operation.** Plan the FtoF like a combat operation. Include the following:
 - Translator integration.
 - Movement — ingress and egress.
 - Security; both sides know planned meetings. Anticipate to be compromised.
 - Contingency/emergency situations.
 - Covert danger signals.
- **Bring Past Notes or Previous Reports for Reference.** This demonstrates interest as well as directs the conversation into chosen areas interest.
- **Introductions.** Introduce everyone in the party and record the names and positions of everyone outside the party who is attending. Collecting information is a key goal of each FtoF meeting.
- **Photos.** Take photographs of the TA (ask permission).
- **Be Sincere.** Apologize in advance for any cultural mistakes that may be made. Reassure the TA that any offense is not intended and ask the TA to inform the party when a mistake is made so attendees may learn. As the FtoF ends, ask what cultural mistakes were made and thank the TA for helping clarify the TA's culture.
- **Restricted Topics.** DO NOT discuss sensitive issues such as religion or other societal practices.
- **Compare Notes.** Immediately after the meeting, discuss what was observed to ensure an accurate understanding of what occurred.
- **Language.** Never assume the TA does not understand English.

(U) Chance Encounters and Contacts

A chance encounter or contact with the TA occurs most often during patrols at the squad, platoon, and company levels. The leader of the unit should conduct the FtoF based upon a pre-planned battle drill to include the following:

- **Security.** Security of the communicator and the TA.
- **Time.** Limit the length of the FtoF; establish a codeword for when it is time to end the meeting.

- **Identify the Local Leader.** Ask who is in charge, and talk to/through that individual only. DO NOT distribute anything to the populace without the local leader's permission.
- **Be Fair and Firm.** Stay in charge and respectful, not rude.
- **Group Size.** Select a maximum of 1-2 people to engage in a FtoF.
- **Take Notes.** Get names of all people contacted, approximate ages, hometown, business/activity, subjects covered, demeanor towards the participants in the FtoF and/or friendly forces, and any particular concerns of the TA.
- **Pledges.** Make no promises that cannot be kept.
- **Establish Rapport.** Offer the TA refreshment such as a bottle of water and move to a comfortable location. Sit if possible.
- **Focus.** Stay on message by knowing what messages the command is focusing on in specific AOs and during specific time periods.
- **Reinforce the Message.** Use any applicable/available printed products (handbills, pamphlets, posters) in order to reinforce the verbal message.
- **Report.** Report all contacts with local leaders up the chain of command to ensure that an accurate picture of the situation is developed.

(U) How to Use Translators

This specifically applies to CAT I (local hire, un-cleared) translators. However, some aspects are applicable to CAT II (cleared for SECRET) and CAT III (cleared for TOP SECRET) translators.

Always remember the translator will be viewed by the local community as the "voice and representative" of the United States and the command. So monitor the translator and keep all aspects of his behavior professional and ethical regardless of his nationality or ethnicity.

(U) General Guidelines

- **Translator Principles.**
 - Speak in first person.
 - Remain nearby when the parties in the FtoF are speaking.
 - Carry a note pad and take notes, as needed.

- Project clearly and mirror the vocal stresses and overall tone of all conversations being translating.
- **Know the Translator.** The lives of the Soldiers may be in the translator's hands. Know the translator's strengths and weaknesses.
- **Treatment.** Always treat your translator as part of the unit. The better the translator is integrated in to the unit, the better the translator's performance.
- **Employment.** Ensure that the translators are used for translation duties only. Using them for other activities may violate their contract. An example of misemployment is using a translator to run errands in town. However, sending the translator to town to coordinate a meeting for a U.S. official is allowed. A good rule of thumb: If the translator is acting as the official voice of the command, the action is legal.
- **Protection.** The translator may be subject to physical harm because of the messages being delivered.
- **Training.** If your translator is allowed to carry a weapon, ensure he can handle it in a safe manner. Range familiarization/qualification as well as knowledge of movement techniques and nuclear, biological, and chemical equipment are highly recommended.
- **Rest.** Allow the linguist rest periods to collect his thoughts, get a drink, etc. Meal meetings are especially challenging for a translator. Make sure that he is allowed to eat during or after the meeting.
- **Uniform.** Translators should be dressed like the troops they are supporting so they can be identified as "friendly" in a combat situation to preclude fratricide. Uniform accessories such as wet weather gear, body armor glint tape, etc., that are common on Soldiers uniforms should be made available to the translator.

(U) Rehearsing with a Translator

- **Check the Translator.** Verify your translator's abilities. To ensure accuracy and security, periodically record your translator, both with and without his knowledge, for quality checks by higher headquarters.
- **Isolate the Translator.** If operational details are briefed to the translator during the mission rehearsal, consider having the translator remain on the base camp until execution. Also, ensure the translator does not have a cellular telephone or other communication device.

- **Rehearse Conversations.** This is especially important with complex, new, or sensitive issues. A rehearsal will help define words the translator may not know and ensure the translator understands the overall message to be conveyed.
- **Provide Feedback.** Make corrections as needed.

Remember, if the translator performs poorly, it affects the TA's perception of the Soldier involved. Look for ways to assist the translator in doing better.

(U) Working with a Translator

- Always maintain eye contact with the person being spoken to and not the translator. The translator is your voice. Communicate through him, not to him. Watch the TA's gestures, eyes, body language, and not those of your translator.
- Speak in short clips. Do not recite a long paragraph and expect the translator to convey the intent. The TA needs to feel like he is conversing with the Soldier and not being lectured. One to two sentences at a time is a good rule.
- Do not use acronyms, slang, and idioms — keep it simple.
- For simple ideas or routine information, the Soldier can feel confident that the translator is capable of delivering the conveyed message as intended by introducing the topic and then expressing confidence in the translator's ability to speak on the Soldier's behalf. End the conversation with closing comments and ask if there are any questions.
- Be cautious about telling jokes — the humor can backfire.

(U) Battle Drills and SOPs

There are situations that may require established battle drills or standing operating procedures that pre-plan information the translator will convey to the local populace. Some possible situations and the type of information that the translators should be prepared to provide are the following:

- **Vehicle Checkpoints.** Explanations of what military forces are doing; questions about where vehicle occupants are going, or do they have weapons; instructions on search procedures for vehicle occupants.
- **Cordon and Search.** An explanation of what military forces are doing; questions about whether the residents have any weapons or have seen any suspicious activities.

- **Detention of a Person.** An explanation of why the person has been detained; the detention process; how the detainee's family can reach the person detained; and how friendly forces humanely treat detained persons.

Chapter 13

Countering Threat Propaganda in the Information Environment

This chapter describes the following:

- How to analyze threat propaganda and its effects on the information environment (IE) in order to determine counter-propaganda measures.
- General characteristics of regional propaganda that may be encountered in these environments.

This chapter is designed to augment doctrine, based on 1st Information Operations Command (Land) tactics, techniques, and procedures for pre-deployment training.

(U) Types of Propaganda

- **White Propaganda.** Propaganda disseminated and acknowledged by the source. Information in white messaging tends to be accurate, albeit slanted.
- **Gray Propaganda.** The source of the propaganda may or may not be identified and the accuracy of the information is uncertain.
- **Black Propaganda.** Credited to a false source and spreads lies, fabrications, and deceptions. It is difficult to detect black propaganda before significant amounts of facts are revealed.

Related to Propaganda: Misinformation and Disinformation

- **Misinformation.** Unintentionally incorrect information. May emanate from virtually any source.
- **Disinformation.** Friendly, neutral, or hostile information disseminated to distort and deceive or influence a target. Includes covert propaganda.

(U) Propaganda Techniques

- **Name Calling.** Using a name or word to connect a person to something negative (for example, Muslim extremists terming Westerners “crusaders”).
- **Glittering Generalities.** Twisting the meaning of a word that has great symbolic value (for example, terming terrorist attacks as a “jihad”).

- **Euphemisms.** Using a milder word to make a situation seem less threatening (for example, “revenue enhancement” to describe a tax hike).
- **Transfer.** Using symbols to associate an agenda with a respected institution (for example, placing disinformation on official letterhead stationery).
- **Testimonial.** Adding credibility to a position (for example, using celebrities to testify on political issues).
- **Bandwagon.** Playing on the desire of people to want to fit in (for example, “7 of 10 workers prefer candidate X”).
- **Fear.** Manipulating peoples’ fears to elicit a behavior (for example, “without jihad, the crusaders will invade your homes”).

(U) Five-Step Counterpropaganda Process

1. Analyze Target Audiences	• Understand the environment – the AO, the inhabitants, the culture, and the adversary
2. Analyze Propaganda	• Establish a collection plan (IRs) • Analyze propaganda using SCAME • Catalog (construct database)
3. Analyze Media Affecting the Environment	• Identify media bias and propaganda in the media • Become aware of media footage or symbology that could be manipulated by the adversary
4. Apply Counter-propaganda Measures	• Compare the propaganda analysis results with the various counterpropaganda techniques and available IO assets; apply appropriate countermeasures
5. Monitor	• Evaluate the effects of counterpropaganda measures

Figure 13-1. Five-step counterpropaganda process chart.

(U) SCAME Analysis

Source, content, audience, media, effects (SCAME) is a technique for analyzing opponent propaganda to determine the impact of an individual piece of propaganda on the IE. SCAME is a vital part of any counterpropaganda process.

- **Source.** Identify the originator or sponsor of the propaganda.
- **Content.** Identify the line(s) of persuasion used — the message and the source’s desired effect.
- **Audience.** Identify the audiences targeted by the source and actually reached by the propaganda. This step is critical to counterpropaganda planning.

- **Media.** Identify the medium used and why that particular medium was selected by the source.
- **Effects.** Determine the impact of the opponent's propaganda on the target audience — try to determine whether the propaganda has caused attitudinal or behavioral change.

(FOUO) Counterpropaganda Techniques

- **Forestalling.** Counter possible lines of persuasion prior to the release of propaganda.
- **Conditioning.** Preemptively shape target audience vulnerabilities prior to exposure to propaganda.
- **Restrictive Measures.** Deny the intended target audience access to the propaganda.
- **Direct Refutation.** Rebutting the propaganda point-for-point.
- **Indirect Refutation.** Question the validity of some aspect of the opponent's argument.
- **Diversion.** Divert attention by presenting more important or relevant themes to the target audience.
- **Imitative Deception.** Alter the propaganda to degrade its impact.
- **Silence.** No response to the propaganda.
- **Minimization.** Acknowledge selected elements of the propaganda while downplaying the importance of the content.

(FOUO) Propaganda in the Middle East

The two dominant themes of modern propaganda in the Arab World are opposition to imperialism and opposition to the state of Israel. Arab nationalism, the cult of a leader, manipulation of Islamic principles, and terrorism have been underlying facets of propaganda since the end of the World War I and the fall of the Ottoman Empire.

- Combines many forms of media, including compact discs, posters, art, graffiti, radio broadcasts, and “night letters.”
- Anti-imperialist.
- Glorifies history, blames the West for problems.
- Uses “David vs. Goliath” parallels, such as urging resistance to “tyrants” using modern weaponry.

- Overstates Arab unity.
- Manipulates Islamist symbology.
- Exploits the Islamic concept of martyrdom.
- Often exploits anti-western sentiments.
- Manipulates and exploits official media coverage.

(FOUO) Propaganda in Southeast Asia

Indonesia is the world's largest Muslim country and fourth largest overall in population. Propaganda targets Indonesian audiences' attempts to overcome the nation's many different ethnicities and languages. The Islamic party Hizb ut-Tahrir is a source of radical Islamist propaganda in the country.

- Forms of propaganda in Kampuchea (Cambodia) denounce the presence of foreigners.
- Intense state-sponsored propaganda (Burma) appeals to nationalist tendencies and the removal of Western commercial interests.

(FOUO) Propaganda in East Asia

This region contains some of the world's most propagandized societies. Most of the countries in the region have widespread information technologies in urban areas. Propaganda has long served as a key tool of the Chinese state, which oversees a huge, populous, and fractious country.

(FOUO) Propaganda in Central Asia

Propaganda in this region reflects the political and historical contexts of the various countries. Propaganda from the radical Hizb ut-Tahrir Islamic group is common in the region. The region's ethnic diversity, political developments, varying degrees of religious influence, and economic development within the context of the information age make it a complex and fragmented target for propagandists.

- Propaganda from Hizb ut-Tahrir advocates (nonviolent) overthrow of the current Central Asian regimes and institution of an Islamic government with Shari'a as the sole source of law.
- Central Asian religious extremist groups exploit martyrdom and anti-imperialist themes.
- Former Soviet Bloc states use state media to combat Islamist messages.

- In Iran, censorship combines with larger-than-life exposure to religious figures (posters, portraits) and rallies to propagate anti-Western messages.

(FOUO) Propaganda in the Caribbean

Cuba is a major player in Caribbean political efforts that use propaganda.

- Anti-slavery liberty movements along the lines of the French Revolution.
- Anti-colonialism and anti-totalitarianism.
- Musical forms, such as calypso and reggae, have been used for political expression and satire.

(FOUO) Propaganda in Latin America

Recently, some governments (Venezuela) have used national channels to spread anti-U.S. propaganda. Other themes include:

- Liberation.
- Desire for self-determination.
- U.S. imperialism.
- Pro-communist, anti-communist.
- Anti-United States.
- Anti-drug.
- Environmental protection.

(FOUO) Propaganda in Africa

The primary lines of persuasion in this region revolve around colonialism or anti-colonialism.

- Bolster one-party rule.
- Support for decolonization and nation building.
- Rally for Western political-military objectives.
- Many messages directed at public health efforts, such as acquired immune deficiency syndrome awareness.
- Genocide has been supported by hate propaganda (Rwanda), which used radio and public rallies as media.

(FOUO) Propaganda in South Asia

Propaganda revolving around Pakistan and India's battle in the Kashmiri territorial dispute is dominant in this region.

- Propaganda is intertwined with education in South Asian madrassas (religious schools).
- Some conservative Indian media outlets have been accused of propagating against Pakistan.
- Glorification of Osama bin Laden.

(FOUO) Instrument of Insurgencies and Guerrillas

Propaganda is a key weapon used by guerrilla and insurgent movements. Although propaganda is used as part of psychological warfare conducted during conventional conflict, its importance is heightened during a low-intensity conflict such as a counterinsurgency.

- In the modern IE, transaction costs associated with media have been drastically lowered; thus, the volumes of propaganda and associated challenges of monitoring it have increased exponentially.
- Emotions and attitudes are crucial factors in the spread of insurgencies and the harboring of insurgents.
- Insurgent and counterinsurgent forces will use lines of persuasion to sway the populace to support each side's objectives.

Chapter 14

Tactical Perception Management

This chapter describes how selected information and indicators conveyed to the local populace can be managed to influence public opinion of friendly and enemy forces.

This chapter is designed to augment doctrine, based on 1st Information Operations Command (Land) tactics, techniques, and procedures for pre-deployment training.

(U) Definitions

There is no doctrine for perception management; however, the following explanations of terms are necessary to understand perception management:

- **Perception Management.** Actions that convey selected information and indicators to a foreign local populace for the purpose of influencing perceptions of friendly and threat forces.
- **Perception.** An interpretation of reality based on observations and information received from the surrounding environment. Perceptions influence decisionmaking and patterns of behavior. For the purposes of perception management, there are three basic types of perceptions:
 - **Positive Perceptions.** Those perceptions the foreign local populace must have in order to support the presence and activities of friendly forces.
 - **Negative Perceptions.** Harmful perceptions among the foreign local populace that result in behaviors that counter friendly activities or support threat activities.
 - **Unintended Perceptions.** Unplanned perceptions among the foreign local populace that result from friendly or threat activity.

(U) Basic Concepts

By managing the perceptions of the foreign local populace, tactical units can gain and maintain the populace's support while denying it to the threat.

- Perceptions do not have to be valid to have an effect.
- Tactical perception management starts with Soldiers who come into daily contact with a foreign population. How Soldiers behave in front of the populace greatly influences perceptions of whether the presence of U.S. forces is legitimate and credible.

- It is easier to build on positive perceptions than to overcome harmful perceptions. One careless act can undermine the effects of future positive actions.
- Legitimacy is based on the populace's perception of reasons for U.S. forces' presence in the country.
- Credibility is based on how the foreign population perceives U.S. forces' motives and promises and whether or not those meet the local population's needs and desires.

(U) Threat Perception Management

The threat seeks to create harmful perceptions about the activities of U.S. forces.

- The threat uses the following:
 - Means and methods very different from those of U.S. forces.
 - Both truth and lies to shape its version of events.
 - The advantage of its knowledge and relationships with the local populace.
- The enemy seeks to foster uncertainty within the populace by manipulating events in a way that:
 - Questions the role and presence of U.S. forces.
 - Portrays itself as acting on the populace's behalf or as being its defender.
- The threat seeks to erode the trust between the foreign populace and U.S. forces by exploiting negative actions by friendly forces. The threat will highlight the following:
 - Civilian casualties and collateral damage.
 - Mistreatment of civilians and community leaders.
 - Disrespect towards cultural beliefs.
 - Misconduct of U.S. personnel.

(U) Friendly Perception Management

The reputation of U.S. forces relies on the actions of tactical units.

- The sum of individual and small unit actions forms the basis for how the population perceives U.S. forces. To be effective, U.S. forces need to build and maintain credibility and legitimacy. The required perceptions can be created by the following:
 - Treating the local populace with dignity and respect.
 - Interact in a positive way with local groups.
 - Responding to needs of the local populace (as possible).
- Unintended perceptions can foster rumors and create uncertainty in the local population about the legitimacy of the mission and intent of U.S. forces.
- Harmful perceptions resulting from negative events will damage U.S. forces' reputation and can create sympathy for the enemy cause. Be aware that cover-ups and slow responses will only make the situation worse.

(U) Populace Perceptions

History and culture provide insight into populace perceptions.

- Positive interaction with the foreign local populace can create the required perceptions that will build a good reputation for U.S. forces.
- To communicate and interact well with the populace, it is necessary to understand the people's history and culture for the following reasons:
 - History explains how the populace will view current conditions and events.
 - Culture provides the framework and context for group and individual relationships and interaction. It is also the lens through which the actions of U.S. forces will be seen by the populace.

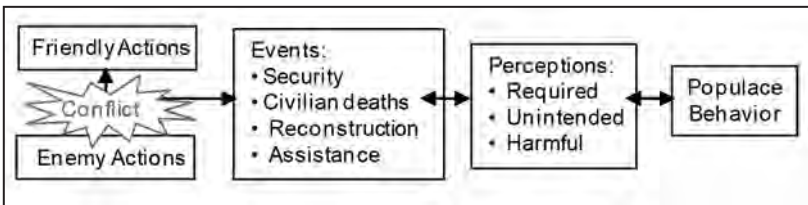


Figure 14-1. Populace perceptions.

(U) Techniques for Perception Management

The following techniques are useful for conducting tactical perception management:

- Communicate with the foreign local populace.
- Treat the populace with dignity and respect.
- Establish and maintain dialogue with local leaders.
- Document friendly and threat activity.

(U) Communicate with Local Populace

Communication is the foundation of effective tactical perception management.

- Listen to the concerns of the foreign local populace.
- Monitor and track populace demonstrations and rallies — it is one way the local populace communicates with the government and U.S. forces.
- Employ select information-related capabilities to tell the unit's story to local media, leaders, and the populace.
- Emphasize the accomplishments of U.S. forces during daily interaction with the local populace. Develop talking points that senior and junior leaders can use to explain these accomplishments.
- Establish professional relationships with local and regional media to avoid mistrust that may lead to negative reporting about friendly forces and the mission.

(U) Treat Populace with Dignity and Respect

Local society is organized for the populace's convenience...not U.S. forces.

- Soldiers do not have to like the culture to understand or use it.
- Don't impose U.S. values on local cultures and norms.
- The local populace reacts to the perceptions of the United States in general, not just U.S. forces assigned to the area.
- Remember, actions speak louder than words. Follow up on promises and agreements.

(U) Establish and Maintain Dialogue with Local Leaders

Multiple actors and entities occupy the operating environment.

- Engage faction leaders to achieve situational awareness and to determine who is supportive, indifferent, or hostile to the U.S. presence and objectives.
- Communicate with faction leaders to understand the intent, motivation, and needs of groups the leaders represent.
- Focus dialogue on concerns and needs of the local populace and how these concerns/needs can be met.
- Ensure consistency between friendly operations and dialogue with the factions.

(U) Document Friendly and Threat Activity

Document operations to tell the story of U.S. forces.

- Document the activities of the following:
 - U.S. forces to build credibility and support for the mission.
 - Threat forces to discredit its actions and ideology in the eyes of the populace.
- Always be accurate and factual to maintain trust and avoid embarrassment.

(U) Small Unit Leader Tips

Tactical perception management starts at the squad and platoon levels.

- Think asymmetrically and ask, “If I were the threat what could, and would, I do to influence the populace’s perceptions?”
- Provide immediate local assistance when practical (i.e., health and welfare, security) — compassionate initiative is a timeless tool, and a U.S. unit may be the only entity capable of providing immediate relief.
- Continue perception management activities even after physical actions and events are concluded to exploit or mitigate long-term effects and consequences.

(U) Influence Principles and Methods

Principles

- **Liking.** If the local populace likes or respects U.S. forces, the local citizens are much more likely to cooperate. To foster these positive perceptions, try to establish commonalities between U.S. troops and the local populace.
- **Reciprocity.** It is human nature to help those who help you. Positive actions and assistance by U.S. forces will often be returned in kind by the local populace, although it may take time to see positive results.
- **Consistency.** Most humans do not like change. Once individuals or groups respond a certain way, they will often do so again in order to avoid change, inconsistencies, or conflict.

Methods

- Try to communicate in the manner and style of the population. Education, age, and gender all affect how tactical units interact with various populace groups.
- Simplify facts into ideas easily understood and familiar to the populace, such as “right and wrong,” “good and evil,” or “legal and criminal.”
- Compare the benefits of friendly actions to the negative consequences of enemy actions. Use examples to illustrate the point; for example, other groups that have improved their conditions by cooperating with U.S. forces.

(U) Perception Management Tracker

- A tool for tracking populace perceptions in the area of operations.
- Helps determine what actions are favorably perceived by the population.

Perception Management Tracker						
Action or Event	DTG	Positive Perceptions	Negative Perceptions	Unintended Perceptions	Indicators	Status
Establish local security station	01/09	US forces working to develop security in the district	None	US forces are here to exploit the people and steal their land	Attacks on security station and local patrols	Red – Daily SAF and IED attacks continue
Collateral damage: civilian buildings damaged	01/09	US forces take great care to avoid unnecessary damage and casualties	US forces have no regard for local populace	None	Riots, negative reports in local media	Green – CMO made mitigation payments

Figure 14-2. Perception management tracker.

Chapter 15

Staff Battle Drills

In the modern information environment (IE), transaction costs associated with the media have been drastically lowered; thus, the volumes of propaganda and associated challenges of monitoring it have increased exponentially. This chapter describes how to develop staff battle drills for information operations (IO) that pre-plan and coordinate collective staff tasks and actions in anticipation of possible threat action or events in the IE. Staff battle drills are designed for specific situations requiring rapid reaction and provide a pre-coordinated response to that situation.

This chapter is designed to augment doctrine, based on 1st Information Operations Command (Land) tactics, techniques, and procedures of pre-deployment training.

(U) Staff Battle Drills

For IO, quick responses to battlefield events and threat action are necessary to beat the threat in the IE and ultimately achieve information superiority.

Battle drills are developed during the planning process; however, the drills are not complete and final courses of action (COAs). Rather, battle drills are pre-developed concepts that anticipate crises. Once the crisis occurs, the battle drill (or prospective COA) can be quickly adjusted to address the realities of the situation at hand.

Battle drills perform the following functions:

- Anticipate likely crisis situations.
- Are based on specific unit missions, tasks, standards, and performance measures.
- Focus on the basics.
- Aid teamwork and cohesion under stress.
- Should be realistic in scope.

(U) Developing Staff Battle Drills

Identify Critical Events. Determine critical events that may result from threat, friendly, or third-party action during the upcoming operation. Focus on events that will either occur in, or affect, the IE and are significant enough to affect the command's mission.

Determine the Purpose. The purpose should clearly describe the operational advantage that IO will provide to the commander.

Develop IO Concept of Support. A concise and easily understandable word picture that describes how information-related capabilities (IRCs) may be employed and what staff coordination must be conducted to employ the assets. The concept must be integrated with the overall operation, when applicable.

Synchronize Tasks and Targets. Develop tasks and purpose, methods and means, and if appropriate, targets for each participating IRC. Include a purpose for each task to explain each asset's part in the operation. If appropriate, identify general target sets for each tasked element or asset.

(U) Critical Events

A military operation is a series of events, planned and unplanned, that requires both friendly and enemy forces to react to a changing situation. Some events are critical to mission success of friendly or threat forces. The following applies to critical events:

- Battlefield events create both intended and unintended effects and may be brought on by friendly, threat, or third-party actions.
- Critical events can be either negative or positive.
- For negative critical events, a battle drill should mitigate the impact of the event on the populace and friendly forces.
- For positive critical events, a battle drill should exploit the event to maximize the positive benefits of the impact to the populace and negative benefits to enemy forces.

(U) Identify Critical Events

To be critical, an event must have the potential to impact mission success. The following are examples of critical events that impact the IE and friendly IO:

- Civilian casualties and collateral damage.
- Displaced persons and refugee returns.
- Fratricide.
- Enemy or friendly violations of FM 27-10, *The Law of Land Warfare*.
- Capture and exploitation of friendly force Soldiers.
- The killing or capture of key enemy leaders.
- Disclosure of the critical information list (CIL) or classified information.
- Hostile propaganda directed against friendly forces.

- Negative media reporting.
- Destruction of key infrastructure.
- Mistreatment or death of a detainee.

Assumptions. The specific time, location, and circumstances of critical events are likely to be unknown. When identifying critical events, also identify any assumptions made about each event.

Likely Friendly Action. It is necessary to determine the friendly forces' likely response to the critical event before defining information superiority.

(U) Determine the Purpose

- Battle drills are designed to respond to a specific situation. Therefore, the situation must be sufficiently defined so the planner can adjust the battle drill's concept to compensate for the differences between the planned and actual situation. This means having a purpose for IO.
- The purpose is expressed as an operational advantage provided to the commander through the control and management of information content and flow in the area of operation. It is achieved through the deliberate generation of effects within the IE by the combined, methodical employment of IRCs directed at specific target objectives.
- After determining the purpose, describe what the operational advantage is that IO will provide to the commander in narrative form.

- The following is an example of a purpose description for a mitigation battle drill:

Event: Disclosure of CIL or classified information.

Target: Enemy.

Purpose: Prevent adversary decisionmakers from taking advantage of sensitive information about the friendly force.

- The following is an example of a purpose description for an exploitation battle drill:

Event: Destruction of key infrastructure by threat forces.

Target: Populace.

Purpose: Decrease populace support for the threat forces.

(U) Develop an IO Concept of Support

The level of detail is determined by how much information is known when the battle drill is created. The IO concept of support should include the following:

- **Assumptions.** List information accepted as “true” in the absence of facts at the time the battle drill is developed.
- **Purpose of IO.** Determine, and then describe, what operational advantage IO will provide.
- **General Scheme for IO.** Use doctrinal concepts and terms to explain how IO will achieve operational advantage. List any IO objectives (if used) and key tasks. Include who will perform each key task and when.
- **Priority of Support.** Designate which subordinate unit or element has priority use of assigned IRCs or external IO and cyberspace operations support teams.
- **Constraints on IO.** List prohibited and directed actions that are expected to affect the IO. Think in terms of information content and flow and the generation of predictable effects within the IE.

(U) Determine Tasks and Targets

Determine Tasks. Consider all IRC assets, maneuver units, and those staff entities such as G-2/S-2, G-3/S-3, G-5/S-5, G-6/S-6, and G-9/S-9 that may have important roles in responding to the battle drill event. Include a purpose for each task to maximize asset initiative, and have supporting elements develop “measures of performance” for the assigned tasks.

Consider the following questions when determining key tasks:

- Are both the threat and the IE addressed?
- Are both human and technological aspects of the IE considered?
- Are information content and flow being affected?
- Are key tasks performed by the right asset at the most effective time?

The following are examples of key tasks:

- Conduct key leader engagement with local government officials.
- Broadcast radio messages.
- Counter enemy propaganda.

Determine Targets. Identify key target sets for each tasked element or asset. Possible targets are civil and political leaders, local populace, and adversary leaders.

(U) Staff Battle Drill Format

There are several different battle drill formats currently in use. The format illustrated in Figure 15-1 has worked well in the field. Modify the format, as needed, to fit the command's needs and situation.

(CRITICAL EVENT)				
<i>SITUATION: Describe the critical event</i>				
<i>ASSUMPTIONS: List assumptions regarding the critical event</i>				
<i>LIKELY FRIENDLY ACTION: List likely friendly force response to the critical event</i>				
<i>IO CONCEPT: Define Operational Advantage provided by IO, General Scheme for IO, Priority of Support, Constraints on the Employment of IO</i>				
Element	Key Tasks	Purpose	Method	Target
<i>List unit or person responsible for the task</i>	<i>What must be done</i>	<i>What the task will do</i>	<i>The means or method to accomplish the task</i>	<i>To whom the task is directed</i>

Figure 15-1. Example battle drill format for a critical event.

(U) Example Staff Battle Drill

INSURGENT-RELATED VIOLENCE				
SITUATION: Insurgent forces attack friendly forces, a friendly third party organization, or an opposing faction (e.g., a bombing, shooting, or mortar attack). The insurgent force is not destroyed during the attack. Friendly forces do not incur any significant casualties.				
ASSUMPTIONS: The insurgent attack does not cause significant friendly casualties.				
LIKELY FRIENDLY ACTION: A response force is deployed to find and destroy the insurgent force. Security operations are conducted in and around the area of attack. If necessary, force protection measures are increased.				
IO CONCEPT: The purpose of this info operation is to gain populace support for counter-insurgency activities. IO assets provide direct support to the response force. PSYOP teams, disseminate print products to the populace near the attack site. Unit leaders and a CA team engages local leaders to gain support for friendly operations. PAO issues a press release to explain the command's position & counter misinformation concerning the situation. Restrictions: PSYOP restricted to preapproved themes. MOE: Increased reporting of insurgent activity by populace.				
Element	Key Tasks	Purpose	Method	Target
MISO	Disseminate print products and radio broadcasts to the populace of villages in & around the attack site.	Reduce populace support for insurgent forces & activities	Handbills and Posters Contract Radio	Local Populace
Civil Affairs	Engage local leaders	Gain support for counter-insurgency activities	Face to Face	Civil Leaders
Unit Leaders	TBD	TBD	TBD	TBD

Figure 15-2. Example of an insurgent-related violence, staff battle drill, reflecting all relevant information.

(U) Example of Abbreviated Staff Battle Drill

Situation. React to collateral damage resulting from coalition force action.

Purpose. Pre-empt enemy propaganda and negative media reporting.

Immediate (on-site) actions.

- Notify commander.
- Document the scene (combat camera photos, etc.).
- Conduct key leader engagement to determine facts and conduct initial mitigation.

Within two hours, perform the following actions:

- Notify battlespace owner.
- Notify local government officials.

- Synchronize IRCs to generate effects within the sub-IE that conveys a public statement of the facts that is consistent with the command narrative; where possible and plausible, leverage the foreign local print, radio, and television media.

Within 24 hours, perform the following actions:

- Conduct key leader engagements with local elders using host-nation partner-unit commanders, coalition commanders, and local government officials.
- Assess damage for possible civil-military operations' (CMO) projects.

After 24 hours, perform the following actions:

- Coordinate for follow-up media coverage and key leader engagements.
- Compensate family, if appropriate, and conduct CMO activities.

References

1. Field Manual (FM) 3-13, *Inform and Influence Activities*, 25 January 2013.
2. Army Regulation 530-1, *Operations Security (OPSEC)*, 26 September 2014.
3. Joint Publication 3-13.4, *Military Deception*, 26 January 2012.
4. FM 3-53, *Military Information Support Operations*, 4 January 2013.
5. FM 3-61, *Public Affairs Operations*, 1 April 2014.
6. Army Doctrine Reference Publication (ADRP) 6.0, *Mission Command*, 17 May 2012.
7. Army Doctrine Publication (ADP) 5-0 (FM 5-0), *The Operations Process*, 17 May 2012.
8. ADRP 3-0, *Unified Land Operations*, 16 May 2012.
9. ADP 3-0 (FM 3-0), *Unified Land Operations*, 10 October 2011.

PROVIDE US YOUR INPUT

To help you access information quickly and efficiently, the Center for Army Lessons Learned (CALL) posts all publications, along with numerous other useful products, on the CALL website (CAC login required). The CALL website is restricted to U.S. government and allied personnel.

PROVIDE FEEDBACK OR REQUEST INFORMATION

<https://call2.army.mil>

If you have any comments, suggestions, or requests for information (RFIs), use the following links on the CALL restricted website (CAC login required): “RFI or Request Pubs” or “Contact CALL.”

**PROVIDE LESSONS AND BEST PRACTICES OR
SUBMIT AN AFTER ACTION REVIEW (AAR)**

If your unit has identified lessons or best practices or would like to submit an AAR, please contact CALL using the following information:

Telephone: DSN 552-9569/9533; Commercial 913-684-9569/9533

Fax: DSN 552-4387; Commercial 913-684-4387

CALL Restricted Website <<https://call2.army.mil>> (CAC login required):

- Select “Submit Observations, Best Practices, or AARs” tab at the top of the page.
- Under “Document Identification,” enter AAR subject in “Subject of Lesson or TTP” block.
- Identify whether or not the AAR is classified in the “Is it Classified?” block.
- Select the “Browse” button by “File to Upload” block and upload the AAR file.
- Enter questions or comments in the “Comments/Questions” block.
- Press “Submit Form” button.

Mailing Address: Center for Army Lessons Learned
ATTN: Chief, Collection Division
10 Meade Ave., Bldg. 50
Fort Leavenworth, KS 66027-1350

TO REQUEST COPIES OF THIS PUBLICATION

If you would like copies of this publication, please submit your request at <<https://call2.army.mil>>. Mouse over the “RFI or Request Pubs” tab and select “Request for Publication.” Please fill in all the information, including your unit name and street address. Please include building number and street for military posts.

NOTE: Some CALL publications are no longer available in print. Digital publications are available by using the “Products” tab on the CALL restricted website.

PRODUCTS AVAILABLE ONLINE

CENTER FOR ARMY LESSONS LEARNED

Access and download information from CALL’s restricted website. CALL also offers Web-based access to the CALL archives. The CALL restricted website address is:

<https://call2.army.mil>

CALL produces the following publications on a variety of subjects:

- **Handbooks**
- **Bulletins, Newsletters, and Trends Reports**
- **Special Studies**
- *News From the Front*
- **Training Lessons and Best Practices**
- **Initial Impressions Reports**

You may request these publications by using the “RFI or Request Pubs” tab on the CALL restricted website. (**NOTE:** Some CALL publications are no longer available in print. Digital publications are available by using the “Products” tab on the CALL restricted website.)

COMBINED ARMS CENTER (CAC) Additional Publications and Resources

The CAC home page address is:

<http://usacac.army.mil>

Center for Army Leadership (CAL)

CAL plans and programs leadership instruction, doctrine, and research. CAL integrates and synchronizes the Professional Military Education Systems and Civilian Education System. Find CAL products at <<http://usacac.army.mil/cac2/cal>>.

Combat Studies Institute (CSI)

CSI is a military history think tank that produces timely and relevant military history and contemporary operational history. Find CSI products at <<http://usacac.army.mil/cac2/csi/csipubs.asp>>.

Combined Arms Doctrine Directorate (CADD)

CADD develops, writes, and updates Army doctrine at the corps and division level. Find the doctrinal publications at either the Army Publishing Directorate (APD) <<http://www.apd.army.mil>> or the Central Army Registry (formerly known as the Reimer Digital Library) <<http://www.adtdl.army.mil>>.

Foreign Military Studies Office (FMSO)

FMSO is a research and analysis center on Fort Leavenworth under the TRADOC G2. FMSO manages and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. Find FMSO products at <<http://fmso.leavenworth.army.mil>>.

Military Review (MR)

MR is a revered journal that provides a forum for original thought and debate on the art and science of land warfare and other issues of current interest to the U.S. Army and the Department of Defense. Find MR at <<http://usacac.army.mil/cac2/militaryreview>>.

TRADOC Intelligence Support Activity (TRISA)

TRISA is a field agency of the TRADOC G2 and a tenant organization on Fort Leavenworth. TRISA is responsible for the development of intelligence products to support the policy-making, training, combat development, models, and simulations arenas. Find TRISA at <<https://atn.army.mil/media/dat/TRISA/trisa.aspx>> (CAC login required).

Combined Arms Center-Capability Development Integration Directorate (CAC-CDID)

CAC-CDIC is responsible for executing the capability development for a number of CAC proponent areas, such as Information Operations, Electronic Warfare, and Computer Network Operations, among others. CAC-CDID also teaches the Functional Area 30 (Information Operations) qualification course. Find CAC-CDID at <<http://usacac.army.mil/cac2/cdid>>.

Joint Center for International Security Force Assistance (JCISFA)

JCISFA's mission is to capture and analyze security force assistance (SFA) lessons from contemporary operations to advise combatant commands and military departments on appropriate doctrine; practices; and proven tactics, techniques, and procedures (TTP) to prepare for and conduct SFA missions efficiently. JCISFA was created to institutionalize SFA across DOD and serve as the DOD SFA Center of Excellence. Find JCISFA at <<https://jcisfa.jcs.mil/Public/Index.aspx>>.

Support CAC in the exchange of information by telling us about your successes so they may be shared and become Army successes.

Center for Army Lessons Learned

10 Meade Avenue, Building 50
Fort Leavenworth, KS 66027-1350



US Army
Combined
Arms Center

"Intellectual Center of the Army"

US UNCLASSIFIED
FOR OFFICIAL USE ONLY