For Official Use Only

MAY 2005

Tactical Commander's Handbook Information Operations

Operation Iraqi Freedom (OIF)

CENTER FOR ARMY LESSONS LEARNED (CALL)
COMBINED ARMS CENTER (CAC)
FORT LEAVENWORTH, KS 66027-1350

For Official Use Only

FOREWORD

This handbook provides the tactical operator, commander, and battle staff with information on planning, executing, assessing, and sustaining information operations (IO). The handbook is based on observations collected in Iraq during July and August 2004 by an IO collection and analysis team (CAAT). The application of this tool is both for training and real-world events the Soldier may encounter in the Iraqi area of operations.

Because Soldiers are primarily warfighters, this handbook emphasizes those concepts key to operational planning for conflict. It provides a basis for Soldiers to understand the relevance of information operations and a planning framework for the implementation of information operations.

The language and organization of information operation concepts continue to evolve and the debate continues at the highest levels. This handbook is a collection of observations, issues, lessons, and best practices from Operation Iraqi Freedom (OIF) and provides Soldiers a warfighter's orientation to information operations. It is for use in training as Soldiers prepare for deployment and operations in Iraq.

Lawrence H Saul

LAWRENCE H. SAUL
COL, FA
Director, Center for Army Lessons Learned

INFORMATION OPERATIONS HANDBOOK

Table of Contents

CENTER FOR ARMY LESSONS LEARNED

Director	Colonel Lawrence H. Saul
Managing Editor	Lon Seglie
Project Analyst	Robert J. Meier
Editors, Layout, and Design	Jenny Solon Valerie Tystad
Cover Design and Graphics	Mark Osterholm
Labels and Distribution	Carrie Harrod

ACKNOWLEDGMENTS: The Center for Army Lessons Learned (CALL) has collaborated with the Department of the Army (DAMO-ODI), Washington Army National Guard Information Operations Group (WA ARNG IO GP), U.S. Army John F. Kennedy Special Warfare Center and School (USAJFKSWCS), United States Military Academy (USMA), Command and General Staff College (CGSC), Vermont Army National Guard Information Operations Training Battalion (VT ARNG IO TNG BN), U.S. Army Field Artillery School, U.S. Army Combined Arms Doctrine Directorate (CAAD), and Combined Arms Center Information Operations Proponent (CAC G7) to prepare and publish this handbook. The collaboration efforts included collection of information operations observations; issues; lessons; and tactics, techniques, and procedures (TTP) in the Iraqi area of operations in order to help save U.S. and coalition lives through efficient and effective application of information operations across the range of military operations.

This information was deemed of immediate value to forces engaged in the Global War on Terrorism and should not be necessarily construed as approved Army policy or doctrine.

This information is furnished with the understanding that it is to be used for defense purposes only; that it is to be afforded essentially the same degree of security protection as such information is afforded by the United States; that it is not to be revealed to another country or international organization without the written consent of the Center for Army Lessons Learned.

If your unit has identified lessons learned or tactics, techniques, and procedures, please share them with the rest of the Army by contacting CALL:

Telephone: DSN 552-3035 or 2255; Commercial (913) 684-3035 or 2255
Fax: DSN 552-4387; Commercial (913) 684-4387
E-mail Address: callrfi@leavenworth.army.mil
Web Site: http://call.army.mil

When contacting us, please include your phone number and complete address.

We solicit your feedback to make this a more useful tool for Soldiers. Please use our Army Knowledge Online (AKO) collaboration Web site:

1. Sign into AKO.

2. Enter this URL into the address line and click "go."
https://www.us.army.mil/suite/portal.do?$p=515

3. You will be taken to the IO TTP Collaboration site.

4. Click on the "Send Feedback" link, approximately ¼ of the way down the page, slightly left of center; this will open a separate "Send Feedback" window.

5. You will see a drop down menu that lists "Help Desk." Select "Page Creator." Click "Continue" and follow the directions to submit feedback to the IO proponent.

Chapter 1

Introduction

A. Operational Environment (OE)
B. What does IO do for me?
C. Doctrine and this handbook
D. What is Information Operations (IO)?
E. What IO is not
F. IO in the Iraqi Area of Operations (AO)

> ***"IO, however, provides a company commander an opportunity to take control of his sector, earning the respect of local officials and citizens."***
>
> ***Infantry Company Commander, Operation Iraqi Freedom***

"IO is not everything, but everything we do has an IO effect."

A. Operational Environment (OE). The Iraqi operational environment (IOE) is characterized by numerous contradictions in the manner U.S. Army units have been configured, resourced, and trained. The U.S. Army is without peer in today's world and is configured, resourced, and trained to execute combat and related operations in a sequential, fluid environment, as ably demonstrated by V Corps in the major combat operations (MCO) phase of operation Iraqi Freedom OIF. See Figure 1-1 below:

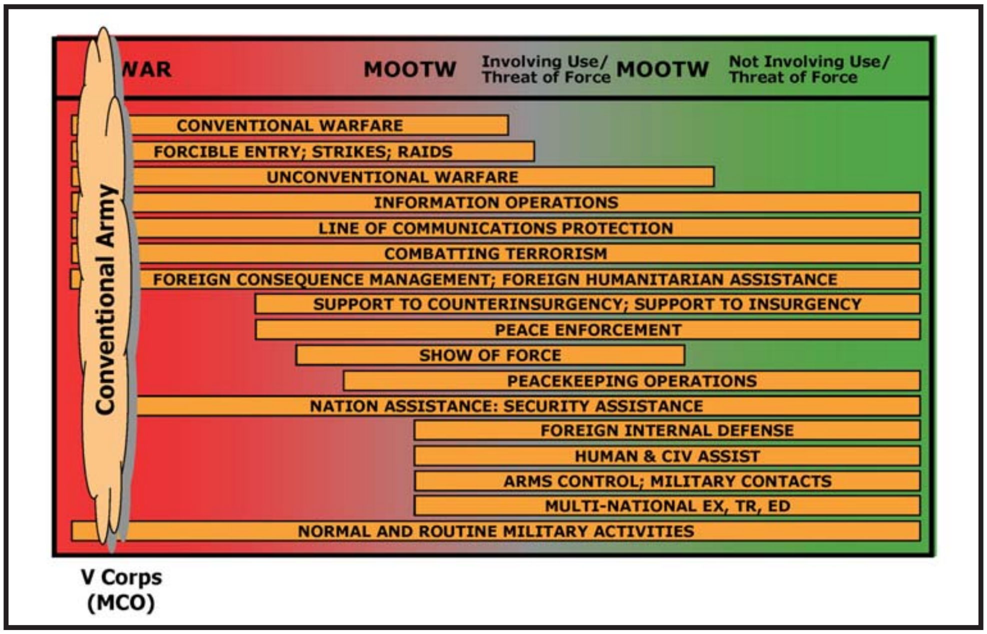

WAR
MOOTW
Involving Use/ Threat of Force
MOOTW
Not Involving Use/ Threat of Force
CONVENTIONAL WARFARE
FORCIBLE ENTRY; STRIKES; RAIDS
UNCONVENTIONAL WARFARE
INFORMATION OPERATIONS
LINE OF COMMUNICATIONS PROTECTION
COMBATTING TERRORISM
FOREIGN CONSEQUENCE MANAGEMENT; FOREIGN HUMANITARIAN ASSISTANCE
SUPPORT TO COUNTERINSURGENCY; SUPPORT TO INSURGENCY
PEACE ENFORCEMENT
SHOW OF FORCE
PEACEKEEPING OPERATIONS
NATION ASSISTANCE: SECURITY ASSISTANCE
FOREIGN INTERNAL DEFENSE
HUMAN & CIV ASSIST
ARMS CONTROL; MILITARY CONTACTS
MULTI-NATIONAL EX, TR, ED
NORMAL AND ROUTINE MILITARY ACTIVITIES
Conventional Army
V Corps
(MCO)

Figure 1-1

The IOE, however, is quite different from the OE for which Army units were configured, resourced, and trained. While combat operations are a part of everyday life for the Soldier in Iraq, the primary mission is to set the conditions, by means of stability and reconstruction operations (S&RO), for an Iraqi government and a populace that is not hostile to the U.S. Not only are these operations different, but they are executed in a much different and complex environment. Units in the IOE operate from fixed bases and conduct numerous operations simultaneously. See Figure 1-2 for post-MCO (PMOC) situation:

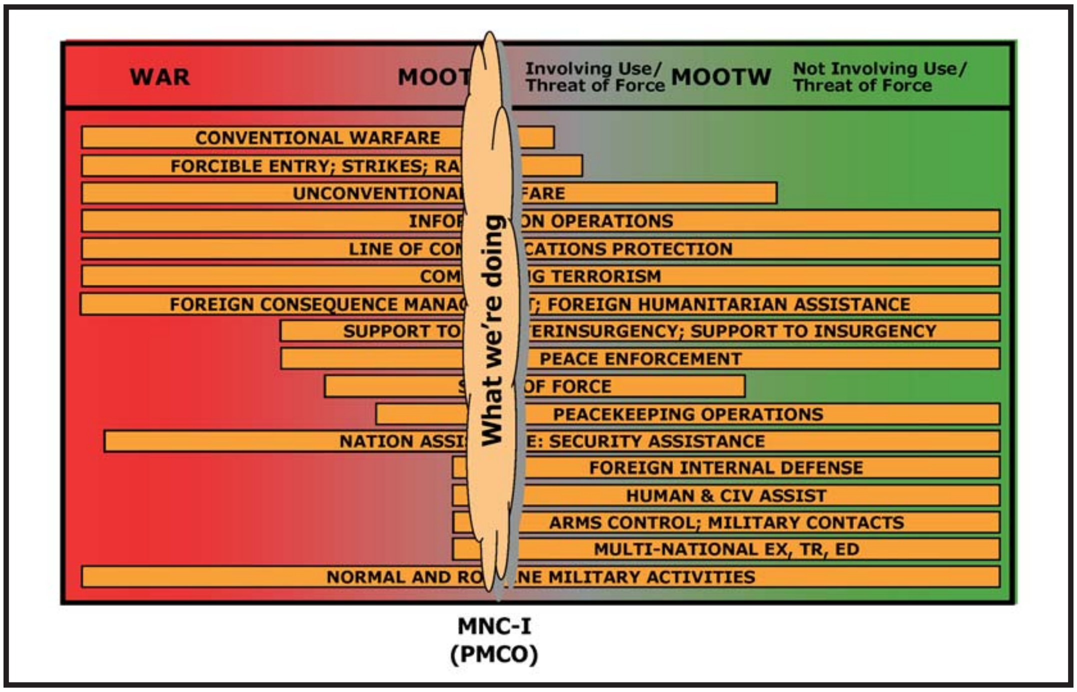

WAR
MOOT
Involving Use/ Threat of Force
MOOTW
Not Involving Use/ Threat of Force
CONVENTIONAL WARFARE
FORCIBLE ENTRY; STRIKES; RA
UNCONVENTIONAL FARE
INFOR ON OPERATIONS
LINE OF COM CATIONS PROTECTION
COM G TERRORISM
FOREIGN CONSEQUENCE MANAG T; FOREIGN HUMANITARIAN ASSISTANCE
SUPPORT TO ERINSURGENCY; SUPPORT TO INSURGENCY
PEACE ENFORCEMENT
S OF FORCE
PEACEKEEPING OPERATIONS
NATION ASSI E: SECURITY ASSISTANCE
FOREIGN INTERNAL DEFENSE
HUMAN & CIV ASSIST
ARMS CONTROL; MILITARY CONTACTS
MULTI-NATIONAL EX, TR, ED
NORMAL AND RO NE MILITARY ACTIVITIES
What we're doing
MNC-I
(PMCO)

Figure 1-2

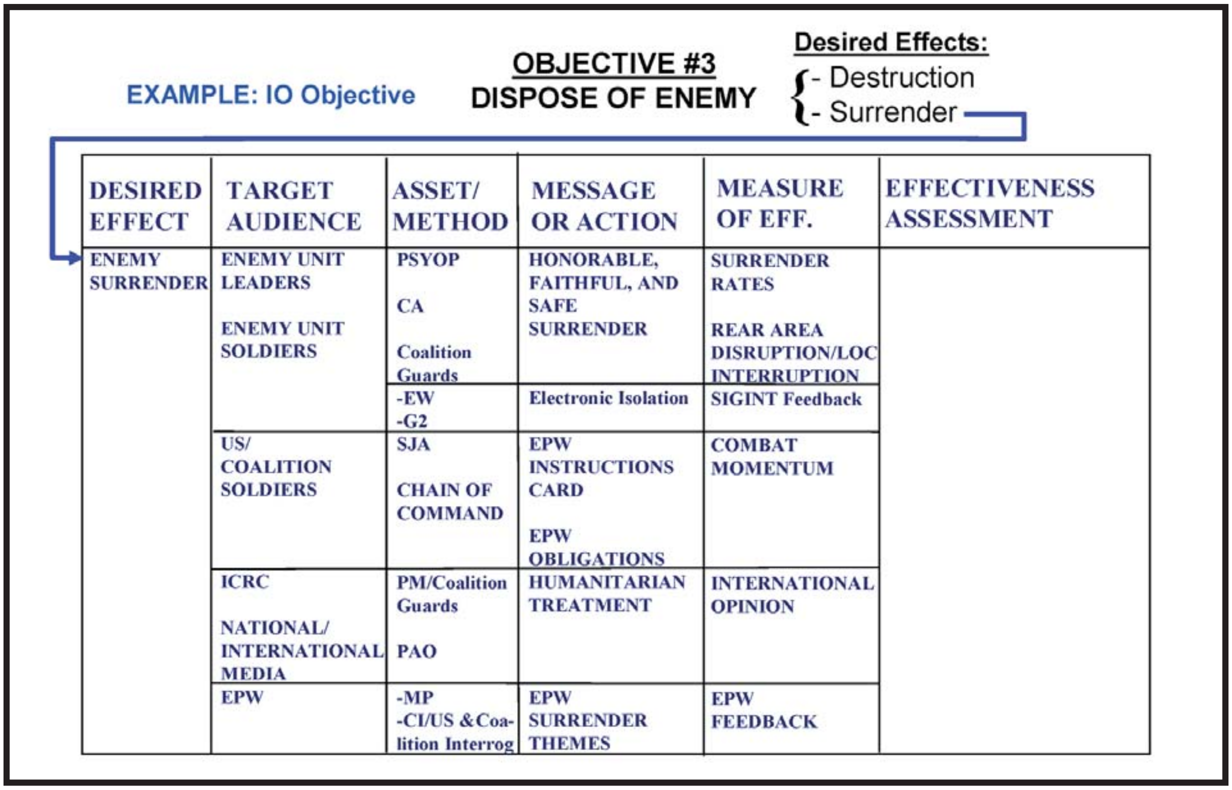
IO is relevant to Soldiers because commanders in Operation Iraqi Freedom (OIF) have found the proper synchronization of information to be the main effort in making up the difference between how we are configured (conventional Army) and how we operate (what we're doing) in this S&RO environment.

B. What does IO do for me? Everything the U.S. Army plans and executes is for the purpose of achieving an effect or effects. Whether it is closing with and destroying an enemy or relating to the local populace, Army units operate to achieve effects. IO assists the commander to shape his environment by achieving effects, both lethal and non-lethal. He achieves effects through the coordination and synchronization of the use of information among all unit activities. OIF has demonstrated that units are more likely to achieve desired effects when information is properly coordinated and synchronized.

> **Example**: A unit commander approved an operation that included a deception component to the plan. The deception component required the enemy to have functional communications for three days or for the duration of the deception, so the enemy could

“intercept” coalition communications that allegedly indicated operational intent. The communications nodes, however, were scheduled for destruction by lethal fires in the next 24 hours which would render the deception plan ineffective. The IO working group (IOWG) synchronized the need for the use of deceptive information in the deception plan, and the destruction of the enemy’s communications was delayed until the deception plan no longer had need for them. The deception plan was effective, and Soldiers' lives were saved as a result.

Example: A unit commander’s intent is to cause the maximum number of enemy to surrender as possible. The staff coordinates and synchronizes the use of information using all available assets and arrives at this objective. See Figure 1-3:



EXAMPLE: IO Objective

OBJECTIVE #3
DISPOSE OF ENEMY

Desired Effects:
- Destruction
- Surrender

DESIRED EFFECT	TARGET AUDIENCE	ASSET/ METHOD	MESSAGE OR ACTION	MEASURE OF EFF.	EFFECTIVENESS ASSESSMENT
ENEMY SURRENDER	ENEMY UNIT LEADERS ENEMY UNIT SOLDIERS	PSYOP CA Coalition Guards	HONORABLE, FAITHFUL, AND SAFE SURRENDER	SURRENDER RATES REAR AREA DISRUPTION/LOC INTERRUPTION	
		-EW -G2	Electronic Isolation	SIGINT Feedback	
	US/ COALITION SOLDIERS	SJA CHAIN OF COMMAND	EPW INSTRUCTIONS CARD EPW OBLIGATIONS	COMBAT MOMENTUM	
	ICRC NATIONAL/ INTERNATIONAL MEDIA	PM/Coalition Guards PAO	HUMANITARIAN TREATMENT	INTERNATIONAL OPINION	
	EPW	-MP -CI/US &Coalition Interrog	EPW SURRENDER THEMES	EPW FEEDBACK	

Figure 1-3

C. Doctrine and this handbook. ***FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures,*** (Nov 2003), defines information operations as “the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making."

Because an underlying theme in most observations concerning IO is the lack of published IO tactics, techniques, and procedures (TTP) at the tactical level, this handbook is configured with information and TTP that have been found to work, whether or not they are published.

Many officers involved in planning IO are not trained in IO. They typically are civil affairs (CA) psychological operations (PSYOP), field artillery (FA), or assistant S3 (AS3) officers who have been detailed to the task. While **FM 3-13** offers an excellent tutorial on planning IO, it does not effectively show TTP for specific IO tasks. This requires IO officers and noncommissioned officers (NCOs) who may or may not be experts in the disparate elements of IO to somehow glean these TTP from data mining the Internet, discussions with peers, or their imaginations. The purpose of this handbook is to provide TTP-level information for the commander and staff, along with suggested planning and synchronizing products.

The use of “IO speak” in this handbook has been minimized because the focus of the handbook is the brigade and battalion commanders and staffs, not the trained IO officer.

D. What is IO?

For commanders, IO:

- Is a tool to influence the use of information to meet your intent in every operation
- Is a horizontal staff synchronization process through all elements of combat power and conducted within the construct of the military decision-making process (MDMP)
- Aligns the use of information by all the unit’s existent functions and operations and focuses on the commander’s intent
- Is both lethal and non-lethal, directed under the S3/G3/C3, and vertically integrated with higher and lower plans and with coalition and host nation (HN) IO efforts
- Synchronizes effects

See Figure 1-4 shows a range of agencies that are normally involved in a successfully integrated IO. At G staff level, these are often assigned special staff officers; at brigade and battalion levels, these are additional duties for designated staff officers.

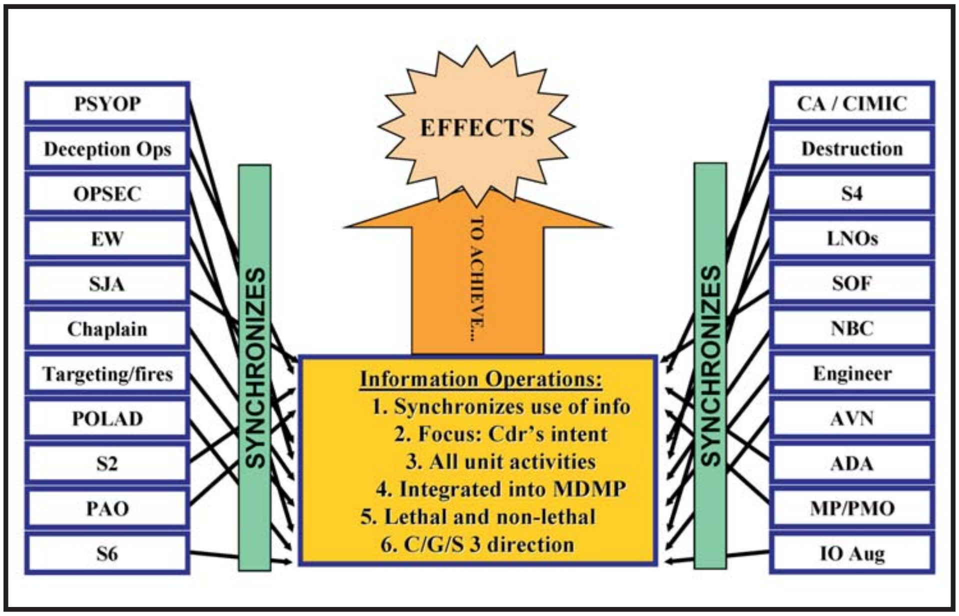


Figure 1-4

In other words, IO coordinates and synchronizes the use of information within all elements of combat power across the spectrum of command and staff activities to achieve effects. See Figure 1-5:

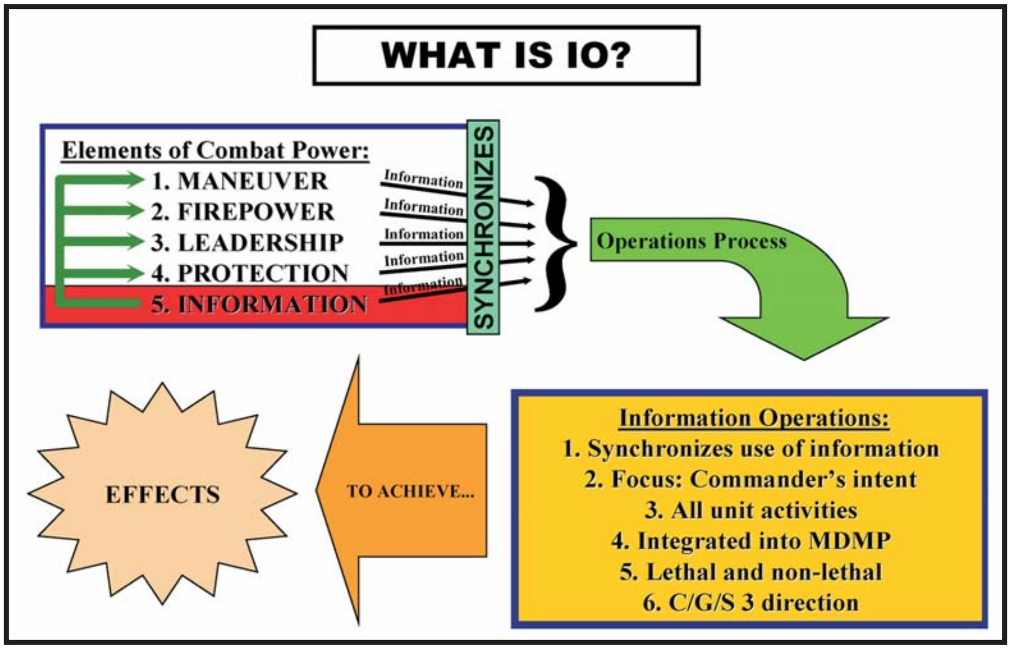


Figure 1-5

FM 3.0 states that commanders combine the elements of combat power - maneuver, firepower, leadership, protection, and **information** - to meet constantly changing requirements and defeat an enemy. Commanders do this by synchronizing the elements of friendly force combat power to create overwhelming effects at the decisive time and place. Massed effects created by synchronizing the elements of combat power (all five elements use information) are the surest means of limiting friendly casualties and swiftly ending a campaign or operation. IO assists you, as the commander, to mass the effects of actions and messages in the information environment to accomplish the mission.

E. What IO is not. IO:

- Is not magic, rocket science, or nuclear fusion
- Does not compete with the MDMP and is not an independent planning activity, nor do staff elements fall under it
- Does not have command and control (C2) of other staff elements (staff elements continue to work for their current boss while synchronizing the use of information through IO to support the commander's intent)
- Is not a separate independent staff element, another C3/G3/S3, or just another staff product
- Does **not** develop separate IO themes and messages; public affairs [PA] and PSYOP are the doctrinal staff elements that transmit themes and messages).
- Is **not** only non-lethal
- Is not another battlefield operating system (BOS)

F. IO in the Iraqi AO. Brigades and battalions plan and execute information operations (IO) continuously in the Iraqi AO. IO had been considered primarily strategic or operational in nature and was, therefore, planned only at the highest levels, theater, corps, and some divisions. This is no longer the case; brigade and below are on the front lines of IO planning and execution. Tactical commanders realize that success (mission accomplishment) often equates to effective employment of IO within their AO. IO must be tailored to local circumstances, area leaders, and the local populace. IO is nested with the overall theater-level IO plan.

While there are no easy solutions for complex IO situations, this handbook provides a sample "way ahead" for the commander and staff. It provides a somewhat detailed discussion of IO at the unit level. It leverages current and emerging doctrine, discusses principles and fundamentals related to IO, and provides a framework for the unit commander and staff to use when planning, executing, evaluating, and sustaining IO.

Chapter 2

Organizing and Executing for Information Operations (IO)

A: Considerations for Brigade and Battalion Staffs
B. Importance of the Iraqi Culture
C. Brigade IO Staff Tasks
D. Battalion IO Staff Tasks
E. Coordination
F. Integrating and Deconflicting
G. Tactics, Techniques, and Procedures (TTP)

"You have to know what is important in the daily life of the average Iraqi - security, services, and jobs."

A: Considerations for Brigade and Battalion Staffs

1. Command Emphasis. Successful IO relies on command emphasis to achieve its integrating and synchronizing effects. Successful brigade and battalion IO includes a member of the command group providing oversight of the IO process. In previous rotations, this oversight has been provided by either the executive officer (XO) or operations officer (S3). Ultimately a command group link to the commander has resulted in successful IO; units without a command group link or command emphasis have been significantly less successful.

2. The critical organic staff positions at the brigade and battalion level are the IO coordinator (IOCOORD), public affairs officer (PAO), IO plans officer, operations security (OPSEC) officer, electronic warfare officer (EWO), chaplain, and civil military operations officer (S5). Psychological operations (PSYOP) support is provided by the supporting PSYOP tactical PSYOP detachment (TBD) (brigade) or tactical PSYOP team (TPT) (battalion). Other essential staff participants are reflected in Figure 2-1.

3. There are normally insufficient staff resources at the tactical level to dedicate entirely to the execution of IO. To address this need, commanders have assigned additional duties to some staff officers and detailed others to support their IO program. Below is a synthesis of how previous commanders have addressed the staffing requirements. An outline of the staff members' duties is listed below.

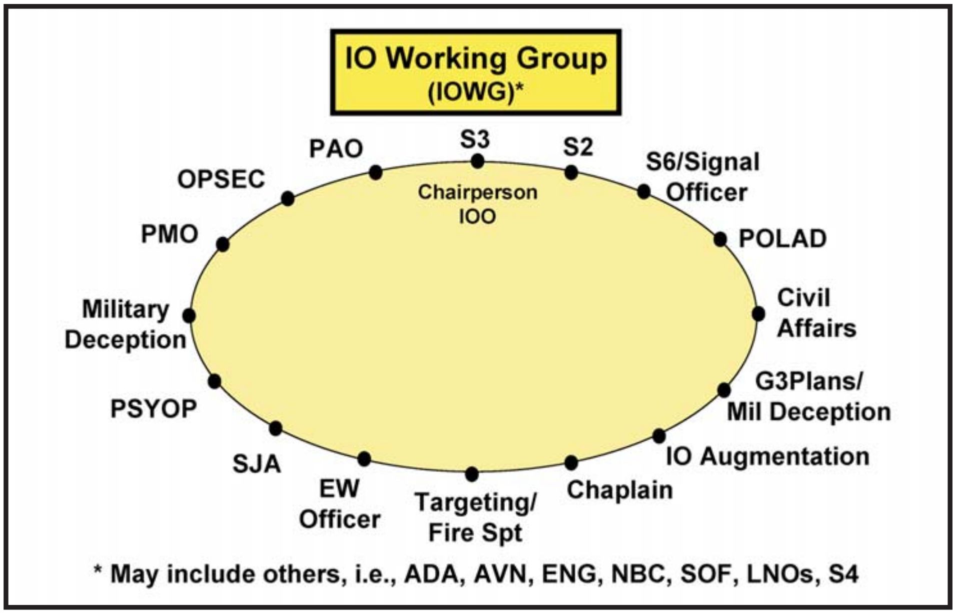


Figure 2-1

B. Importance of the Iraqi Culture

1. The importance of culture in determining the effects of IO cannot be underestimated. IO effects such as deny, degrade, influence, and disrupt C2 or the flow of information can be difficult to measure; however, the means to achieve the effect is more apparent. It requires some understanding of basic human behavior and the culture you are dealing with, as well as the efforts of an adversary to counter your efforts. Culture is defined as:

- The gate through which all people receive, process, and act on information.

- Learned and shared attitudes, values, and ways of behaving in a society.

- Customs, folkways, manners, mannerisms, etiquette, behaviors, body language, gestures, celebrations, milestones, dress, outlooks, perceptions, and thought patterns.

- History, art, myths, legends, and heroes.

- Language, world view, beliefs, behavior, attitudes and values, religion, technology, law, politics, education, history, social organization.

VIGNETTE:

During a movement along a main supply route (MSR), a convoy of five U.S. military vehicles moved through a sparsely populated area and observed a bus driving in the opposite lane strike a young goat herder. The commander stopped the convoy and dispatched two of his combat medics to render immediate first aid; the commander, local tribal leader, and the boy's uncle decided to evacuate the boy for required urgent medical care.

The young boy was rushed into the emergency room with a broken leg and internal damage. The two natives asked the commander why such an important man as himself would take the time to help a goat herder, a boy with very little value. He answered "I am a guest in your country and if this had of happened to someone in my family then I would have wanted someone to help them." This concept seemed strange to them, that an American would spend his time on a boy from his tribe, whom he did not know nor to whom he was related. The boy was treated and released to the commander and family, with a follow-on appointment the following Saturday. The commander provided them with a ride back to their family.

The following Saturday morning the U.S. military completed the follow-up appointment and delivered some clothes, sporting equipment, and miscellaneous supplies to the five-family compound. Women and teenage girls greeted the returning child and U.S. Soldiers. This is very unusual and showed that the village leaders had a measure of trust in the Soldiers. This was a direct effect of the incident with the boy.

The command wanted to insure they leveraged (as a non-lethal effect) the goodwill developed as a result of the humanitarian aid. The deputy commander wanted to insure that a follow-up hasty village assessment was conducted and that subsequent CA/civil military operation (CMO) projects (e.g. water well, school repair, and medical clinic) were planned and conducted. The humanitarian aid incident and the subsequent CA/CMO efforts directly supported several information operations and effects based targeting objectives (e.g., facilitate national government).

This incident fully illustrates how integration of a non-lethal effect (CMO) within effects based operations (EBO) both supports and enhances the IO campaign plan and assists the commander to achieve his desired combat objectives. There are second and third order effects of the humanitarian aid and subsequent CMO actions. As a non-kinetic effect, some percentage of the commander's relative combat power was preserved because the single event provided a stabilizing catalyst, thus minimizing security requirements along the MSR.

2. Comparison of U.S. and Iraqi cultures. The following table is a very generalized summary of key differences between U.S. and Iraqi culture.

U.S. Basic Values	**Iraqi Basic Values**
Doing	Being
Change and action	Stability and harmony **with discussion**
Individualism/independence/self-reliance	Belongingness, interdependence, reliance upon others

Example: "Mission first, people always"	***Example:*** Relationships come first, business is secondary **follows**
U.S. Interaction Norms	**Iraqi Interaction Norms**
Competition **individual**	**Group competition** cooperation
Verbal **directness**	Verbal and non-verbal
Impersonal	Personal
Example: Winning is everything. Time is money	***Example:*** **Maintaining status** The process is as important as the end product. "Let's drink tea."
U.S. Social Structure	**Iraqi Social Structure**
Individualistic	Collective
Nuclear family	Extended family
Achieved status	Ascribed status
Example: "I did it my way." "Self-made millionaire."	*Example*: An individual's value is determined by their family heritage, tribe, etc.
U.S. Psychological Orientation	**Iraqi Psychological Orientation**
Psychology of abundance	Psychology of scarcity
Need for achievement	Need for affiliation
Weak uncertainty avoidance	Strong uncertainty avoidance **social order**
Guilt (internal)	Shame (external)
Examples: Abundance. "The world is my oyster." Guilt. Comes from within; does not rely on external judgments.	***Examples:*** Scarcity. Life is a zero sum game. Anything my neighbor gets is something I cannot have. Shame. Depends on getting caught. Derived from others perceptions of you.
Culture, Communication and Conflict, Dr. Gary Weaver, pp. 75-76	

3. Iraqi cultural environment characteristics.

> ***"History, Geography, and Culture are the surest predictors of the future.***
> ***Robert Kaplan***

Iraq as a sovereign nation is a 1920s creation of the Western powers. The concept of Iraqi nationality and loyalty to the Iraqi state is not strongly rooted among many of the inhabitants of Iraq. The people of Iraq are made up of a number of different religious and ethnic groups. The three main groups in order of size are Arab Sh'ia Muslims, Arab Sunni Muslims, and Kurds. Smaller groups include Turkomans, Assyrians, Chaldeans, Yezidis, and Druze. Most Iraqis view their identity as first the family tribe or clan they belong to and then Shi'a, Arab Sunni, Kurd or whichever of the above groups they were born into. Feelings of loyalty to the Iraqi state generally are strongest among Arab Sunnis. The generalizations below may be useful, but tactical leaders must understand such generalizations are not accurate for all individuals and group. Successful tactical leaders must understand the cultural operating environment of their particular AO and tailor their IO to suit the people.

- **History:**
  - º What is now Iraq was:
    - ∗ One of the birth places of human civilization.
    - ∗ Home to the Sumerians, Bablyonians, and Assyrians before the time of Christ.
    - ∗ The center of Islamic civilization from 680 AD-1258 AD. During this time Islamic civilization was the most advanced civilization in the world, far in advance of the West.
    - ∗ The birthplace of Shi'a Islam as a separate sect of Islam. Iraqi Shi'as view their history as one of near continuous oppression at the hands of the Sunnis.
    - ∗ Not considered a nation until 1920 and was ruled as three distinct provinces: Mosul, Baghdad and Basra.
  - º Between 1921 and 2003, Arab Sunnis held most of the political power in Iraq.
    - ∗ Many Iraqi Arab Sunnis view their post 1920 history as struggle to assert the Iraqi state's independence from Western control and regain their ancient position as leader of the Arab world.
    - ∗ Many Iraqis, who are not Arab Sunnis, view their modern history as a story of discrimination and often persecution at the hands of Arab Sunnis.

- º Many Sh'ia and some Kurds feel that the U.S. encouraged them to rebel against Saddam Hussein after the 1991 Gulf War and then withheld expected support, which they believe permitted Hussein to slaughter them.
- º Saddam Hussein's regime was one of the most brutal dictatorships of the post World War II era. Iraqis were frequently executed for statements and actions viewed as critical of the regime.

- **Geography:** The varied geography of Iraq contributes to various styles of living and work activities among the people of the different regions.
    - º North is mountainous
    - º West and southwest are largely barren desert
    - º Southeast is a marshy river delta
    - º Central corridor is a plain divided by the Tigris and Euphrates rivers and numerous canals.
    - º Iraq has the second largest proven oil reserves in the world and has more water resources than most countries in the Middle East.
- **Culture**: Each sect have separate and distinct cultures with some points of commonality:
- **Ethnic Groups**:
    - º Arab Sh'ia Muslims
    - º Arab Sunni Muslims
    - º Kurds
    - º Turkomans
    - º Assyrians
    - º Chaldeans
    - º Yezidis
    - º Druze
- **Religion**: Plays a preeminent or at least very important role in the identities and behavior of each of these groups.

- **Characteristics**:

  Family:

  - ∗ All the cultures of Iraq place a high emphasis on the importance of the family and extended family. Many Iraqis value the reputation and well-being of their family above personal achievement. Some groups also have strong clan and tribal loyalties.

  - ∗ Within families and extended families, older members exercise strong authority over younger members and males over females.

- **Social**:

  - º Personal relationships are valued over impartial adherence to a set of principles and are the basis of cooperation. Rarely can effective business take place if a personal relationship has not been established

  - º Most groups are very conservative about social interaction between unrelated males and females.

  - º Honor and shame are the strongest factors shaping behavior. Affronts to honor must be avenged.

  - º Many Muslims reject ideas about rules for society and the structure of government if these rules originate from non-Muslims.

  - º Many Iraqis agree with the Arab proverb that “1000 years of tyranny is better than one day of anarchy” and are willing to tolerate a repressive government that ensures order.

  - º Many Iraqis do not consider themselves to have rights or responsibilities to the government or state. If they are well connected (having *wasta* in Iraqi terms), they will exploit the power, influence, and wealth of the state. If they are weak or not well-connected, they fear government and expect it to exploit or terrorize them.

  - º One common expectation among most Iraqis is that government will maintain law and order, though most Iraqis expect the state to do this without their individual participation

  - º Many Iraqi groups feel that personal and group possession of weapons is the only sure guarantee against aggression by rival groups (other tribes, Shia vs. Sunni, Arab vs. Kurd etc.).

  - º Iraqis tend to follow news of political events very closely. Rumors and “conspiracy theories” often receive much attention and carry great weight in the minds of many Iraqis.

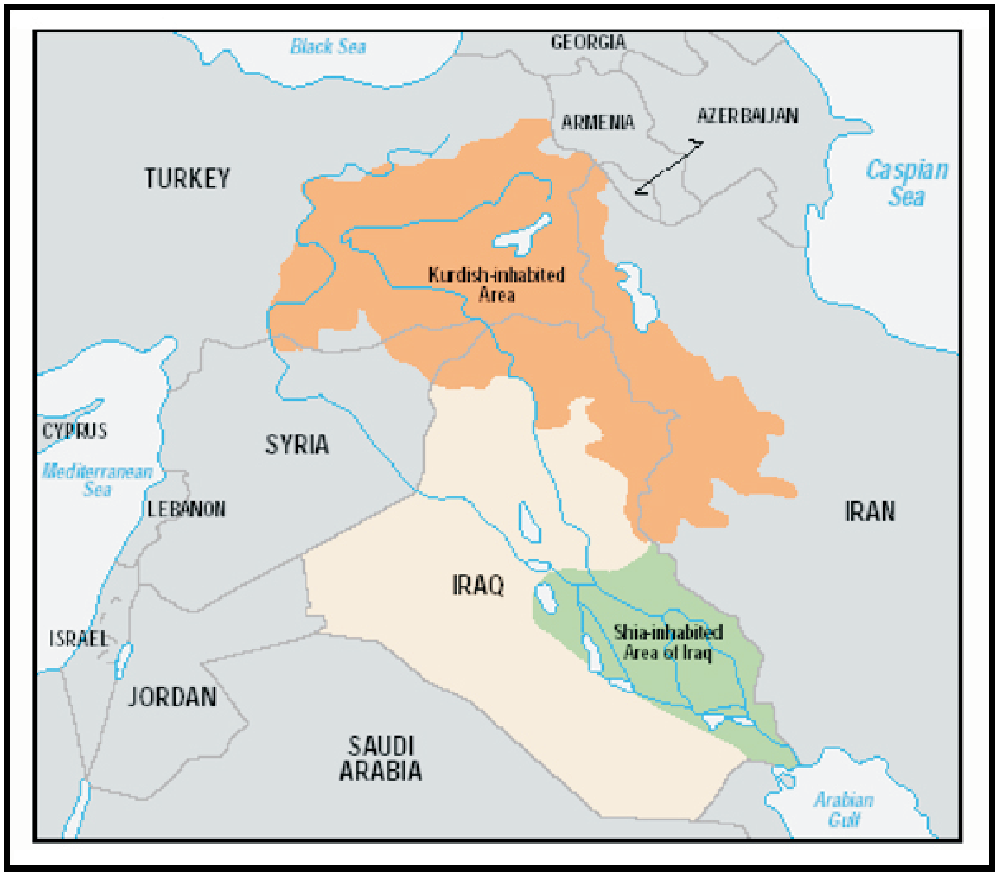


Figure 2-1

4. Tactical leaders' critical cultural knowledge. These are cultural questions every tactical leader should ask themselves. If they do not know the answer, they should seek assistance in getting the answer.

- What is your local area of operations (AO)? What is your area of interest (AI)?
- What is the local peoples' basic world view? Their world view is shaped by their learning and experience in the following areas:
  - Religion
  - Language
  - Beliefs
  - Education
  - Law

  - º Social Organization
  - º Government

- Answers to the following questions can help create a better understanding of the world view of the people in your area of responsibility (AOR):

  - º What things are the people in your local area willing to die for? Being aware of what people are will to die for will give you insight into what there are willing to fight for. If the mission is to foster positive relations, this insight will allow you to distance your Soldiers from areas sensitive to flare ups, i.e., the locals are willing to die for family honor, do not do things that will bring dishonor to the family.
  - º What is the basic social structure of the of your local AO? Is the prime unit the family, clan, tribe, neighborhood, village, political party, religious congregation, or a combination of these? Understanding the social structure will allow you to identify the local power brokers.
  - º Who holds the social, political, economic, and religious leadership in your local area? Do they have an armed following? If yes, what are the size, training, equipment, and loyalty of this following?
  - º Who are the "protectors" (armed citizens, clan or religious militia, police, and army) for the basic social unit (family, clan, tribe)?
  - º What is the religious affiliation of the local people in your area? To what extent are the local people in your area influenced by religion in daily life? What are the dynamics and structure of the local religious leadership?
  - º Do the people in your local area have loyalties, dependencies, or connections (family, clan, tribe, ethnic group, religious sect) that cross outside the boundaries of your AO?
  - º Are there cultural, religious, or ethnic fracture lines in your local area? What are the points of friction between the groups?
  - º How do people earn their living in your local area?
  - º What is the primary legal industry (agriculture, manufacturing, etc.) and what, if any, illegal activities provide significant income (smuggling, drug trafficking, robbery/banditry, black marketeering, etc.). Which of the illegal activities are considered socially acceptable, tolerable, or are habitually overlooked by law enforcement?
  - º What percent of the people are unemployed? What percent do not have basic necessities: drinkable water, food, shelter, clothing, food? Is unemployment a significant problem? If so, do people have difficulty acquiring basic necessities: water, food, shelter, clothing?

- º How, when, and where do the people buy and sell or acquire goods and services, especially essentials such as food, water, fuel, medicines and medical care, clothes, seed, livestock, building materials, vehicles, vehicles repairs?

- º What are the patterns of influence and corruption? What services require payment of bribes, and who receives the payments?

- º What are the points of social etiquette, customs, and mores that can either enhance or harm your acceptability and effectiveness with the people of your local area?

- º How do the people of your local area get their information or news? Which sources have credibility among the local people? How do rumors and conspiracy theories start and spread among the people? What is your feedback loop to know what the people are *really* thinking and saying?

- º What is the most credible source of news/information for the people? Do local elites value a different source?

C. Brigade IO Staff Tasks

1. Information operations coordinator (IOCOORD)

- Advises the commander on IO effects in the context of planned lethal, and non-lethal activities in support of tactical operations. Focuses on the status of friendly, neutral, and adversary IO capabilities and vulnerabilities.

- Ensures IO effects are integrated into operations planning and the resulting operations order (OPORD).

- Ensures that IO actions (performed by assigned or augmenting IO assets) are coordinated, integrated, and synchronized with the brigade plan/order and that division receives IO feedback.

- Obtains and processes relevant information and intelligence to achieve IO situational awareness (SA). Provides IO SA information input to the common operational picture.

- Ensures the IO element performs required staff coordination for IO support from higher headquarters (HQ) and to subordinate units.

- Provides assessments of IO situation and capabilities to support the ongoing military decision-making process (MDMP).

2. IO plans officer

- Integrates IO into the MDMP in support of higher command's IO program.

- Produces OPORD/fragmentary order (FRAGO) and other planning material to support the synchronization of IO across the brigade.

- During wargaming, represents the action, counteraction, and reaction of friendly, neutral, and hostile forces

- Ensures that both offensive and defensive IO tasks are included in planning.

3. PAO

- Conducts media analysis within the brigade AOR.
- Supports media inquiries and visits.
- Adapts higher talking points to the command's AOR. Plans and integrates PAO activities with the rest of the IO team.
- Conducts local media engagement.

4. Operations security (OPSEC) officer

- Conducts periodic OPSEC awareness training in units within the command.
- Develops and posts OPSEC awareness products.
- Conducts periodic OPSEC assessments and conducts remedial training to address deficiencies.
- Integrates OPSEC posture with IO to protect friendly vulnerabilities.

5. Electronic warfare officer (EWO)

- Plans and supervises execution of electronic operations and equipment.
- Collects, evaluates, and prepares reports on threat capabilities.
- Coordinates activities to ensure EW equipment is updated, maintained, and available.
- Monitors division for updates to countermeasures to protect friendly operations.
- Ensures friendly use of EW does not conflict with friendly operation of the electro-magnetic spectrum.

6. S5

- Coordinates CMO projects with IOCOORD, PAO, military police (MP), and engineer (ENG).
- Tracks CMO conducted by brigade and battalions.
- Develops and tracks measures of effectiveness (MOE).
- Reports project status and MOE indicators to division.

7. Command, control, communications, and computer (C4) officer. (The S6 is the staff officer for all C4 matters.) IO-related responsibilities include:

- Provides a representative to the IO cell.

- Provides IO instructions in the C4 operations annex.

- Directs the actions of subordinate net operations.

8. Net operations (NETOPS) officer. (The NETOPS officer integrates mission information applications with information system [INFOSYS] and communications and computer operations of the warfighting information network.) The NETOPS components are:

- **Network management**. Provides commanders with the ability to review and manage their networks to support ongoing IO and to adjust or reallocate network capabilities.

- **Information dissemination management**. Capability to provide a managed flow of relevant information based on the command's missions.

- **Information assurance (IA)**. Includes issuing plans, orders, and policies that minimize the vulnerabilities of information, INFOSYS, and networks consistent with the defense-in-depth concept. Its goal is to protect and defend INFOSYS and networks against exploitation, degradation, and denial of services.

9. Chaplain. In the Iraqi operating environment, chaplains are key members of the IOWG. They have education, skills, and experience to improve U.S. effectiveness in operating in the Iraqi cultural environment and in conducting perception management operations. Major subordinate command (MSC) staff officers all stated that the MSC assistant chaplain was their most valuable advisor on issues of how to deal cross-culturally with Iraqis. The chaplain brought much more than simply the cultural perspective to the IOWG; the chaplain brought the interrelated cultural-religious perspective, which is a broader, more dynamic view of the Iraqi populace than simply historical-cultural information. This perspective speaks to the "who, what, when, where, and why" as it pertains to the ethical framework of the Iraqis and the stark contrasts of the Iraqi culture with our Western culture. The effect on the IOWGs was dramatic. The IOWG members used this perspective-changing information in the development of IO related actions (all IOWG members) and themes and messages (PAO and PSYOP).

The world view of many Iraqis is shaped and animated by Islam, and many chaplains have extensive insight into Islam through training in world religions. Others, as a result of their biblical studies and, sometimes, travel, have extensive knowledge of Middle Eastern history, geography, and cultural customs.

Chaplains often aid the "atmospherics" in dealing with Iraqis. Some Iraqis oppose U.S. operations because they represent American culture. To these Iraqis, American culture, based on what they have seen in American movies and television, is godless and immoral. By accompanying leaders on meetings with Iraqis, chaplains help dispel this view.

- Chaplains are valuable in the planning and implementation of information operations perception management efforts and should be employed as advisors for cross-cultural communication.

- Chaplains can be invaluable members of the IOWG by providing the members with the drastically different cultural-religious perspective of the populace, among whom our Soldiers must relate and operate.

D. Battalion IO Staff Tasks

1. IOCOORD

- Advises the commander on IO effects in the context of planned lethal and non-lethal activities in support of tactical operations. Focuses on the status of friendly, neutral, and adversary IO capabilities and vulnerabilities.

- Ensures IO effects are integrated into operations planning and the resulting OPORD.

- Ensures IO actions (performed by assigned or augmenting IO assets) are coordinated, integrated, and synchronized with the brigade plan/order and that brigade receives IO feedback.

- Obtains and processes relevant information and intelligence to produce IO SA. Provides IO SA information input to the common operational picture.

- Ensures the IO element performs required staff coordination for IO support from higher HQ.

- Provides assessments of IO situation and capabilities to support the ongoing MDMP.

2. IO plans officer

- Integrates the capabilities and vulnerabilities of IO into the MDMP in support of the division IO program.

- Produces OPORD/FRAGO and other planning material to support the synchronization of IO across the battalion.

- During wargaming, represents the action, counteraction, and reaction of friendly, neutral, and hostile forces.

- Ensures both offensive and defensive IO tasks are included in plans.

3. PAO

- Conducts media analysis within the battalion AOR.

- Supports media inquiries and visits.

- Plans and integrates PAO activities with the rest of the IO team. Adapts division and brigade talking points to the command's AOR.

- Conducts local media engagement.

4. OPSEC officer

- Conducts periodic OPSEC awareness training in units within the command.

- Develops and posts OPSEC awareness products.

- Conducts periodic OPSEC assessments and conducts remedial training to address deficiencies.
- Integrates OPSEC posture with IO to protect friendly vulnerabilities.

5. EWO

- Plans and supervises execution of electronic operations and equipment.
- Collects, evaluates, and prepares reports on threat capabilities.
- Coordinates activities to ensure EW equipment is updated, maintained, and available.
- Monitors brigade for updates to countermeasures to protect friendly operations.
- Ensures that friendly use of EW does not conflict with friendly operation of the electro-magnetic spectrum.

6. S5

- Develops CMO projects in coordination with the IOCOORD.
- Develops MOE for CMO projects.
- Tracks CMO projects and MOE and keeps the brigade S5 informed.
- Plans and executes local contracting and purchasing in accordance with (IAW) battalion needs.
- Provides MOE feedback to the IOCOORD.
- Supports the IO intent in preferential selection of contacts and purchases.

7. Chaplain. In the Iraqi operating environment, chaplains are key members of the IOWG. They have education, skills, and experience to improve U.S. effectiveness in operating in the Iraqi cultural environment and in conducting perception management operations. Major subordinate command (MSC) staff officers all stated that the MSC assistant chaplain was their most valuable advisor on issues of how to deal cross-culturally with Iraqis. The chaplain brought much more than simply the cultural perspective to the IOWG; the chaplain brought the interrelated cultural-religious perspective, which is a broader, more dynamic view of the Iraqi populace than simply historical-cultural information. This perspective speaks to the "who, what, when, where, and why" as it pertains to the ethical framework of the Iraqis and the stark contrasts of the Iraqi culture with our Western culture. The effect on the IOWGs was dramatic. The IOWG members used this perspective-changing information in the development of IO related actions (all IOWG members) and themes and messages (PAO and PSYOP).

The world view of many Iraqis is shaped and animated by Islam, and many chaplains have extensive insight into Islam through training in world religions. Others, as a result of their biblical studies and, sometimes, travel, have extensive knowledge of Middle Eastern history, geography, and cultural customs.

Chaplains often aid the “atmospherics” in dealing with Iraqis. Some Iraqis oppose U.S. operations because they represent American culture. To these Iraqis, American culture, based on what they have seen in American movies and television, is godless and immoral. By accompanying leaders on meetings with Iraqis, chaplains help dispel this view.

- Chaplains are valuable in the planning and implementation of information operations perception management efforts and should be employed as advisors for cross-cultural communication.

- Chaplains can be invaluable members of the IOWG by providing the members with the drastically different cultural-religious perspective of the populace, among whom our Soldiers must relate and operate.

E. Coordination

1. **Strength of IO and the IO Team.** When connected and employed effectively, the strength of the entire IO effort will be strengthened and effective.

- Commander provides direction, emphasis, interest, focus, and his intent.

- XO or S3 functions as the command group link.

- IOCOORD takes the lead for the IO staff.

- IO augmentation supports the IOCOORD and provides the experience and expertise to guide and support IO throughout the process.

- Unit staff sections (EW, S6/CNO, PSYOP, military deception [MILDEC], OPSEC, PA, S5/CA/CMO, physical destruction, information assurance, physical security, S2, counterdeception, counterpropaganda, and others) officers/elements operate within their functional lanes to integrate and synchronize IO throughout the operations process.

2. **Organizational Staff Relationships with the IO Process**

- **S1**

    º Can establish a population count of local villages/towns and identify changes in population numbers and demographics (age, sex, main occupations, number of fighting age males) on a monthly basis.

    º Can track locals interested in translation support and their availability.

- **S2**

    º Monitors enemy forces communications: ultra high frequency (UHF), very high frequency (VHF), cell phone systems, commercial, couriers, signaling mirrors, etc.

    º Looks at the civilian populace communications: cell phone systems, hard line phones, radio, TV (satellite and antennae), and newspapers.

- º Monitors the international media (satellite TV, radio, and print) for pro- or anti-coalition effects.
- º Should track and report enemy propaganda events: night-letters, recruiting efforts, posters, and graffiti. Be aware of movement of enemy propaganda/recruiting teams within or through the AOR. What is the EW capability and availability, and what will be its effect?
- º Should look at developing a green/amber/red/white format for reporting local levels of cooperation (white is unknown at present).

- **IOCOORD**
  - º Plans, coordinates, and supervises OPSEC and MILDEC.
  - º Integrates PSYOP into IO and planning and considers product dissemination.
  - º Identifies and disseminates subjects for command information to task force (TF) Soldiers.
  - º Tracks PSYOP/IO product dissemination (who, where, when, how many, which product, local national [LN] reaction).
  - º Identifies potential messages specific to AOR and coordinates with the tactical human intelligence team (THT).
  - º Tracks themes, objectives, and messages emphasized by higher headquarters.
  - º Emplaces and tracks bulletin boards and coordinates with Iraqi security forces (ISF)/Iraqi police (IP) as well as THT for local national (LN) reaction.
  - º Requests products from higher PSYOP.
  - º Recommends mission-specific products for higher production.
  - º Tracks messages being broadcast by friendly Peace radio.
  - º Identifies and tracks enemy propaganda efforts with the S2.

(**Note:** Related activity support to the IOCOORD would be combat camera (COMCAM) to identify opportunities, request support, and attach COMCAM Soldiers to subordinate units based upon mission and COMCAM troops available. PAO would coordinate for media imbeds (journalists), identify to higher PAO potential success stories, and collect all available print media for analysis. CMO would identify Class X for distribution requirements and reporting: where, when, who, what, and how much. CMO would identify reactions from the local populace; identify specific requirements by village; provide support to cooperative leaders and withhold support from uncooperative leaders; track CMO projects, dollars spent, location, effect; and build a report for the battalion commander.)

- **S4**
  - Resources to support CMO.
  - Establishes unit basic load (UBL) of humanitarian daily rations (HDRs); bases activity upon surge and daily requirements.
  - Procures and stores HDRs.
  - Requests Class X supplies through higher headquarters.
  - Collects and distributes sundry pack excess.
  - Maintains humanitarian assistance (HA) kits.
  - The medical staff would normally be a part of CMO and should be coordinated with the IO plan. The medical staff would:
    - Conduct an AOR-wide analysis of endemic illnesses: tuberculosis (TB), hepatitis (HEP), goiter, etc. and develop and track a program to provide medical support to meet the intent of the battalion commander.
    - Schedule clinics and inoculations of locals in coordination with the battalion commander, battalion IOCOORD, and company commanders.
    - Request medical supplies to support civil military assistance (CMA).
    - Conduct “tailgate CMA” in support of battalion combat operations.
  - Develop/track “local needs” matrix for 3/6/9 months out.
  - Conduct local medical training (including feasibility of training local midwives).
- **Engineer** staff responsibilities, like medical operations, need to follow an IO objective. These activities might include:
  - Conducting and tracking a road repair analysis.
  - Determining the feasibility of repairing ground lines of communication (GLOC) to increase task force mobility as well as increase LN mobility.
  - Identifying and storing excess construction material for delivery through ISF/IP to local cooperative leaders.
- **Company commanders** can assist with IO at the local level by:
  - Conducting village assessments and reporting initial assessments and changes through the IOCOORD to the battalion commander.
  - Establishing a presence as the single point of contact (POC) for all activities within their assigned company AOR.

- Developing rapport with cooperative LN leaders and establish dominance over uncooperative leaders through leveraging CMO/CMA and access to higher resources.

- Identifying the type and requirement for CMO/CMA within villages

- Facilitating, through the IOCOORD, nongovernmental organization (NGO) support within supportive villages

- Tracking and reporting, through the IOCOORD, CMO projects to the battalion commander.

F. Integrating and Deconflicting

1. Brigade

The brigade commander has the tools and assets available to achieve his desired effects on an enemy or populace. To synchronize these tools and assets, he must organize the brigade staff for efficiency. If this is not done, the brigade staff will become a network of stovepiped entities, each moving out on a different azimuth.

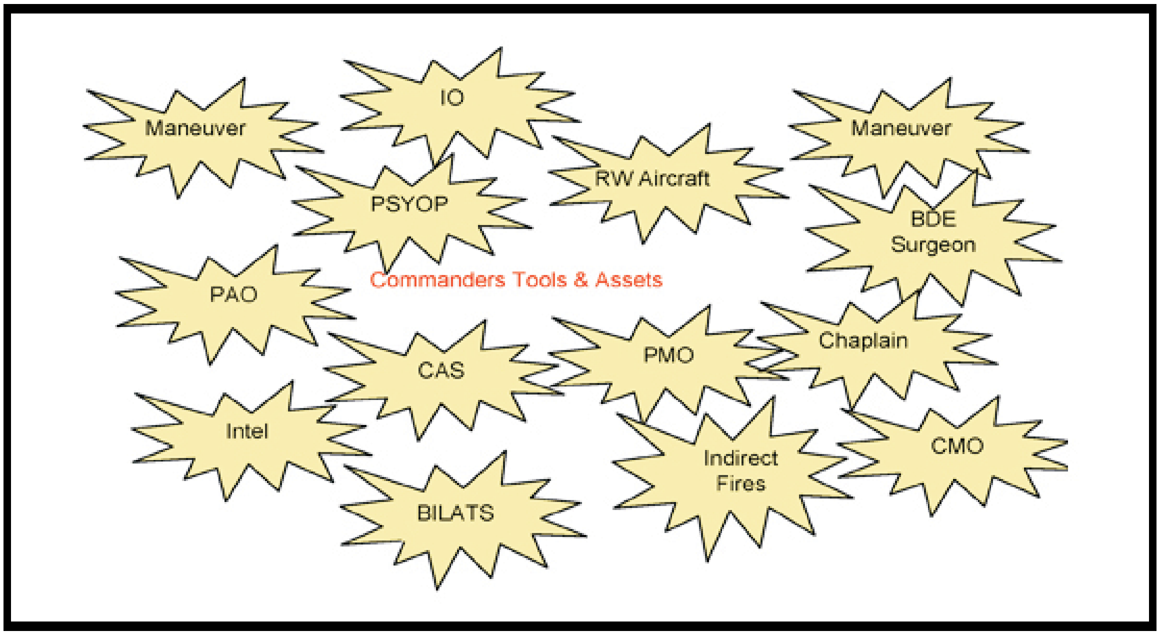


Figure 2-1

Training environments have seen brigade tactical operations centers (TOCs) composed of multiple, seemingly independent cells. It is not unusual to see a current operations cell, a plans cell, a separate project coordination cell (PCC), and a separate effects coordination cell (ECC) or fires and effects coordination cell (FECC). Each of these cells are so independent that orders or instructions sent to subordinate units are not synchronized to achieve the commander's desired effect. All too often they conflict with each other. To correct this, brigade TOCs organize under two overarching cells, plans and current operations. As overall managers and staff section supervisors, the duties and responsibilities of the brigade XO and S3 remain valid. Due to the intensity of operations, it is not uncommon and entirely appropriate for the commander to direct the S3 to focus his efforts on current operations, while the XO focuses on planning future operations. The S3 task organizes within the section with available officers to manage the various staff coordinating cells to accomplish the mission.

PSYOP tactical PYSOP detachment (TPD) is task organized to support the BCT. The TPD commander wears dual hats. As the TPD commander, he provides command and control (C2) for all PSYOP forces attached to or under operational control (OPCON) of the brigade and is responsible for the planning, integration, and monitoring of all tactical psychological operations (TACPSYOP) within the brigade AOR. As the PSYOP staff officer, his responsibilities include:

- Advising the brigade commander and staff on the psychological effects of brigade operations on the indigenous population.
- Serving as the commander's resident staff expert on the indigenous culture and psyche.
- Assisting the S-3 and IOCOORD in the planning and coordination of operations aimed at influencing, informing, deceiving, disrupting, delaying, degrading, or destroying the adversary's means of command, control, communications, computers, and intelligence (C4I) and IO
- Developing PSYOP objectives that support brigade information operations and higher headquarters PSYOP objectives.
- Writing the PSYOP appendix to the brigade OPORD.
- Recommending brigade-specific PSYOP plans and programs to higher headquarters.
- Coordinating with higher headquarters for print, audio, audiovisual, and aviation support for brigade PSYOP operations.
- Monitoring and assessing the effectiveness of PSYOP.
- Monitoring and assessing indigenous demographic, cultural, and political trends within the population.
- Identifying and monitoring enemy propaganda and its sources and recommending actions to mitigate the effects of misinformation.
- Planning and synchronizing aerial loudspeaker and leaflet drop operations in support of brigade operations.
- Identifying and leveraging indigenous media sources, including print, radio, and television, to support division and brigade PSYOP/IO/public affairs (PA) operations.

The staff judge advocate (SJA), a special staff officer, is responsible for providing situational understanding of the legal environment in which the brigade operates. The SJA anticipates the legal implications of expected actions under international law and U.S. law, and the potential perception of those actions based upon the HN legal system. Understanding local legal systems will allow the SJA to forecast the likely actions of enemy forces and potentially available avenues of influencing others to either support the U.S. mission or not resist friendly activities. The SJA works in conjunction with CA to restore or support judicial functions in a local government.

The PCC is responsible for resourcing, prioritizing, and executing CMO to achieve the commander's desired effects.

Level 1 (**s**ewage, **w**ater, **e**nergy, **a**cademics, **t**rash, **m**edical , **s**ecurity [SWEAT-MS]) is the basic life support requirements of the population. Level 2 (**c**ommunications, **r**eligion, **e**conomy, **g**overnance [CREG]) is secondary to Level 1 and is focused on as time and resources become available. As with Maslow's hierarchy of needs, until the Level 1 requirements are adequately established, SWEAT-MS elements are the BCT's priority.

LEVEL 1 (SWEAT-MS) Sewage, Water, Energy, Academics, Trash, Medical , Security

LEVEL 2 (CREG) Communications, Religion, Economy, Governance

The CA officer (S5), a permanent staff member, establishes and supervises the PCC. The S5 and the CA Team Bravo (CATB) team leader are the principal advisors to the commander on CMO. The S5 ensures each COA effectively integrates civil considerations (the "C" of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations [METT-TC]). The CA officer considers not only tactical issues, but also combat support (CS) and combat service support (CSS) issues. HN support and care of displaced civilians are of particular concern. The CA officer's analysis considers the impact of operations on public order and safety and protection of culturally significant sites. If the unit does not have an assigned CA officer, the commander assigns these responsibilities to another staff member.

CATB is task organized to support a BCT in current operations. As with the PSYOP team, these teams have proven to be an invaluable combat multiplier. The CATB operational focus is on the civil center of gravity (COG) and on establishing, maintaining, influencing, and supporting the commander's interaction with government organizations, NGOs, and international organizations.

The engineer coordinator (ENCOORD) is the commander of the engineer unit supporting the BCT. The assistant brigade engineer (ABE) is a permanent staff member who, in the absence of the ENCOORD, acts as an liaison officer (LNO) to the brigade commander and staff. In an environment where units are conducting combat operations and stability operations and support operations simultaneously, the ABE's role in the PCC is to contract or coordinate/task out military troop projects within approved CMO initiatives and track the progress of ongoing projects. The ABE's other vital role is to assess supply routes and nominate targets based on enemy activity on supply routes. Additionally, the ABE provides terrain data and geospatial information to aid in the analysis of enemy operations. The ABE utilizes reach-back capability to the National Mapping Agency and the Corps of Engineers to coordinate for products and professional expertise.

The provost marshal officer's (PMO) role in the PCC is to provide, in coordination with the CATB, assessments to the command on civil defense and local police. Based on assessments and the ground tactical plan, the PMO develops recommendations to improve civil defense and local police. The PMO advises the command on the proper handling of both combatant and noncombatant detainees. In conjunction with CA, the PMO establishes liaison with the local police to assess the local law enforcement system's ability to deal with the types and categories of noncombatant detainees for eventual prosecution. Additionally, the PMO provides route assessment to the ABE.

The medical support officer provides the PCC with an assessment and project recommendations on civilian medical facilities and general populace health within the brigade AOR.

The comptroller or resource manager (RM) is a position that must be filled to accurately account for funds used for CMO. The RM tracks the amount and sources of funding available to the brigade. The RM briefs available funding amounts and limitations as well as amounts already obligated to specific projects or operations.

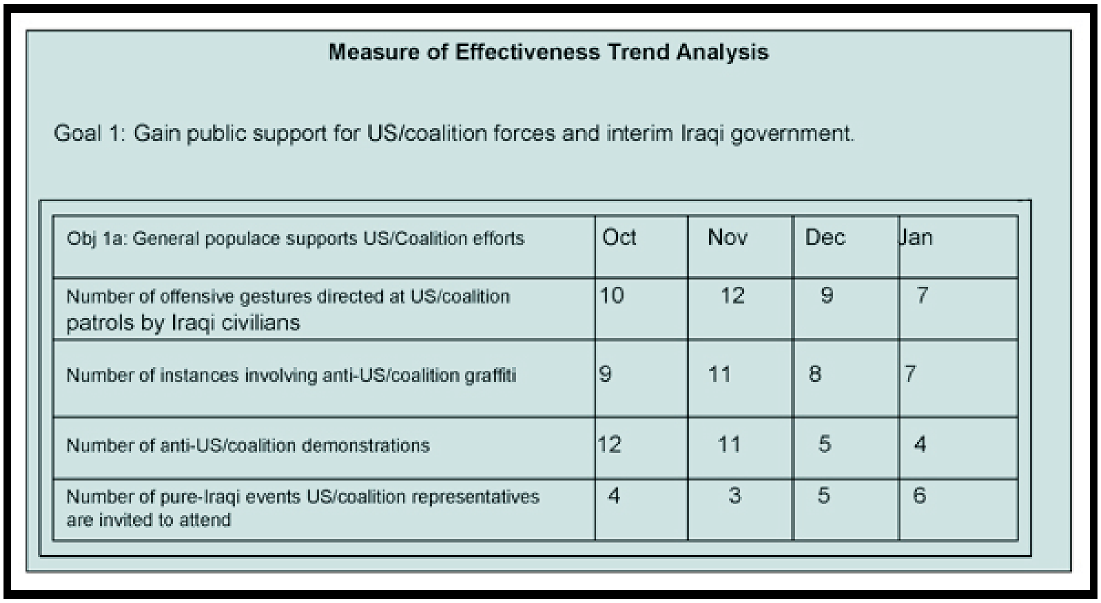
2. **Battalion**

Given the vast amount of terrain and populace a battalion commander must manage, IO becomes critical to accomplishing their complex missions. First, it provides commanders the ability to focus actions and messages to achieve battlefield effects - the end state on an adversary or populace. Second, it provides a method to plan future operations focusing on achieving an objective that are proactive and holistic in countering the enemy. Developing holistic plans designed to achieve a desired effect allows the TF commander to organize all assets in time and space, massing lethal and nonlethal elements of combat power, and forcing the enemy to become reactive. Current TF structure requires a modification in the way the commander and staff think. Commanders and staffs plan, execute, and assess fully integrated operations, using all elements of combat power to achieve overwhelming effects.

Understanding the dynamics associated with continuous combat and stability operations and support operations; realizing the information from every element executing an operation; and shifting focus from the enemy to effects on threats, populace, and civil/tribal leaders are fundamental to achieving success on today's battlefield. They are the paths to accomplishing the theater commander's campaign plan.

In the current environment, IO is central to the concept that every action taken or not taken sends a message to the population, insurgents, and external actors. Whether active or passive, such messages generate behavioral responses. Knowing this, units continuously evaluate and shape their words and actions to ensure they support operations designed to achieve the desired effect. Popular support and proper military action are complementary and feed off each other. Good operations, including nested CMO, IO, and military operations, generate popular support and accomplish the mission set forth in the campaign plan.

At the battalion level, bringing together the efforts of the battalion fire support element (FSE), civil affairs team alpha (CATA), S5, TPT, PAO, and SJA will provide critical resources for the commander to focus CMO, fires, and IO to support maneuver operations.



Measure of Effectiveness Trend Analysis

Goal 1: Gain public support for US/coalition forces and interim Iraqi government.

Obj 1a: General populace supports US/Coalition efforts	Oct	Nov	Dec	Jan
Number of offensive gestures directed at US/coalition patrols by Iraqi civilians	10	12	9	7
Number of instances involving anti-US/coalition graffiti	9	11	8	7
Number of anti-US/coalition demonstrations	12	11	5	4
Number of pure-Iraqi events US/coalition representatives are invited to attend	4	3	5	6

Figure 2-2

Patrol debriefs are an invaluable source of information that provide enormous feedback on daily activities throughout the entire battalion's AOR and its interaction among the populace or with the enemy. Debriefs should be formulated to answer commander's priority intelligence requirements (PIR), specific information requirement (SIR), and specific operational requirement (SOR). At the battalion level, debriefs are so important that the battalion TOC should track them carefully, making sure every patrol is debriefed, and the debrief is analyzed and passed to higher headquarters. This is not a small task and it cannot be ignored. Within the common operating environment (COE), every element leaving a forward operating base (FOB) should be considered a combat or reconnaissance mission. During the processing and analysis of patrol debriefs, both the S2 and the ECC provide a separate but equal analysis of data. The S2 examines debriefs from an enemy and populace perspective, and the ECC examines the data to assist in gauging the progress the TF is having in regards to the campaign plan.

3. **Company**

Execution begins and planning ends at the company level. Company commanders focus on issuing orders, verifying pre-combat checks and pre-combat inspections are performed to standard, controlling operations, and ensuring debriefs are conducted after every mission. When the battalion issues orders, the company commander receives the task, purpose, and SIR/SOR for each mission. The company commander's role is to ensure each mission is executed, the purpose achieved, and SIR/SOR are answered to focus future battalion and brigade operations. Given the fact that a company has no staff, the company commander should turn to his traditional effects coordinator, the fire support officer (FSO), to help manage these new IO tasks.

The traditional role of the company fires support team (FIST) to coordinate lethal fires in support of a maneuver company has evolved to include coordination of both lethal and nonlethal effects. The company FIST coordinates nonlethal effects by developing SOI, tracking Level 1 (SWEAT-MS) and Level 2 (CREG) CMO projects, implementing specific information operation themes and messages and tracking their effectiveness, and acting as company PAO. In addition, FISTs integrate nonlethal combat multipliers such as CATA, TPTs, and human intelligence (HUMINT) teams. Company FISTs are organized to execute lethal effects.

Current trends show company headquarters FSEs are not manned adequately to conduct 24-hour operations. The FSE also lacks the tools and systems to effectively conduct the full range of military operations (ROMO). They must brief and debrief patrols, track SOI, and maintain their capability to deliver lethal effects on a 24-hour basis.

Experience has shown all convoys are combat operations and must be briefed and debriefed along with all other maneuver-centric patrols or operations. A company will have multiple SOIs to track and communicate within its AOR. The traditional method of operations used by company FISTs in a non-stability operations and support operations environment is overwhelmed. Company FSEs must operate like a battalion FSE or effects cell.

The company FSO works with the company commander during operations to successfully accomplish all company essential effects tasks. While the maneuver commander is responsible for integrating lethal, nonlethal, and maneuver, the FSO must understand the scheme of maneuver as well as the company commander understands it. On the basis of the commander’s guidance, the FSO develops his effects plan and presents it to the commander for approval.

Company operations need to mirror battalion operations. Standing operating procedures (SOPs), tools, and systems to gather and manage information need to be in place to meet requirements from battalion. There is a need to have a dedicated lethal and nonlethal cell at the company command post (CP). Without this element, critical information is not tracked, gathered, or managed in the detail required to be successful in combat operations and the stability operations and support operations environment.

The company must analyze the intelligence, surveillance, and reconnaissance (ISR) plan and determine the company’s collection requirements, and then brief those requirements (along with the talking points and MOE) during the mission brief to focus patrols on gathering specific information critical to the planning and refinement at battalion and brigade. FSE themes, messages, and MOE need to be posted in the company for every leader and Soldier to view along with PIR and SIR/SOR.

In today's environment, there are several different missions a company is expected to conduct simultaneously. See Figure 2-3:

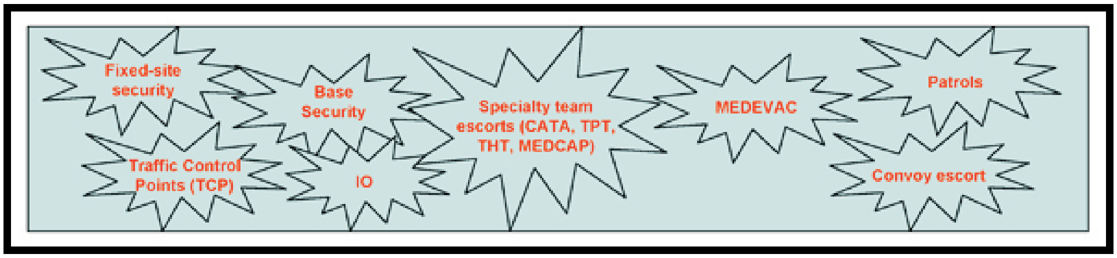

Fixed-site security
Base Security
Specialty team escorts (CATA, TPT, THT, MEDCAP)
MEDEVAC
Patrols
Traffic Control Points (TCP)
IO
Convoy escort

Figure 2-3

A matrix tool is needed to assist the company in tracking patrol operations as well as tracking maneuver and the different missions they are currently executing. An example of a tracking matrix tool is shown below.

COMPANY TRACKING MATRIX							
Element	Mission	DTG start	DTG end	Objectives	SOR/SIR	Brief	Debrief

Figure 2-4

It is imperative that the company conducts patrol briefs with all elements executing missions. Patrol briefs provide focus to the patrol on gathering specific information that may answer PIR or IO indicators. Patrol briefs should follow a prescribed format. An example of a patrol brief format is shown below.

PATROL BRIEFS

- PIR, SIR/SOR
- Copy of MOE (indicators)
- Pertinent info from previous patrol
- Any specialty teams attached and mission
- Specific indicators to observe and report (propaganda, negative hand gestures, throwing objects)
- Non-lethal target status
- Current CMO project status
- Previous patrols' activities (promises)
- Target folder review
- Themes and messages
- Talking points

Figure 2-5

Patrol debriefs are the preferred method for seizing "ground truth." Debriefs should be conducted upon completion of the patrols and involve all Soldiers in the patrol. The debrief should focus on answering SIR/SOR. MOE extracted from the patrol debrief should be forwarded daily to the battalion for review and utilized during the combat synchronization meeting. The current status of CMO projects should be debriefed and updated as well. An example of a CMO Project Tracking Matrix is shown below.

TOWN:	UNIT:	POC:	DTG:		
SYSTEM	ISSUE	ACTIONS	STATUS	CONTACT	PROMISED DUE DATE
SEWAGE					
WATER					
ELECTRICITY					
ACADEMICS					
TRASH					
EMPLOYMENT					
MEDICAL					
SECURITY					

Figure 2-6

It is imperative that CMO projects are tracked in detail at company level. The SWEAT-MS (including employment) tracking matrix is a valuable tool in tracking vital infrastructure and systems and providing the company commander and battalion staff with an accurate picture of the status, contacts, actions taken at company level, and promised date for completion. It assists the battalion staff with established priorities and a focus within the AOR.

G. Tactics, Techniques, and Procedures

1. Information flow

To gain information superiority, commanders rely on ISR, information management (IM), and IO. The synchronization of these activities allows commanders the ability to see first, understand first, and finish decisively. Bottom-fed information comes in many forms. CA assessments, PSYOP assessments, battalion task force commander assessments, bilateral negotiation records, and patrol debriefs are a few. Taken together and analyzed by the staff, they paint a picture for the commander. Staffs must have systems in place to collect this information, update staff estimates, and present this information to the commander in the form of a mission analysis brief. Once staffs and Soldiers understand the paradigm shift of becoming a bottom-fed organization and emplace functional systems to collect such information, they will recognize the importance of IO. These systems enable information superiority. They are critical in allowing the commander to visualize, describe, and direct actions within the brigade or battalion AOR.

2. Planning

Include the higher HQ goals and/or objectives within the unit's mission statement as well as in the key tasks and end state of the commander's intent. By doing this, leaders provide subordinates the use of these effects as the basis for initiative.

A key to effective planning is a clear understanding of the decisive operation. Defining the decisive operation in today's complex environment requires commanders to describe the effect desired against an actor (enemy, local leader, or civil population). To define the decisive operation, commanders must:

- Determine the actor (or group of actors) representing the greatest threat to fulfilling the campaign plan.

- Describe the decisive operation as a "what" (desired effect), not a "who" (identifying the unit to accomplish the decisive operation). For example, a commander could say, "The decisive operation is the identification and neutralization of insurgent C2 cells."

3. Information Operations Working Group (IOWG). The following are attributes and characteristics of functional IOWGs. IOWGs can be informal at brigade and battalion level.

- **Command emphasis.** The commander must support and direct the efforts of the IOWG.

- **Meeting purpose and tone**. The purpose of the IOWG is to coordinate and synchronize specific actions with specific IOWG members. It is not a tasking meeting. IO officers who use the IOWG to task IO elements without input from those elements risk misusing IOWG members. Coordination and synchronization will not occur in an environment where IOWG members feel alienated.

- **Due outs**. The meeting should identify "due outs," proposed supporting actions, members take back to their sections for discussion and/or planning and execution, with a defined date and time when the staff section must report feasibility or progress.

- **Sample meeting flow**:

    - Status of ongoing projects (review of MOE and status report on due outs).

    - Statement of new problem, commander's guidance/estimate, or next phase of the IO plan.

    - How can IO support?

    - How might each activity support?

        - What is currently being done by each member's section?

        - What new/different/modified actions might be taken?

    - Consensus on possible courses of action (COAs).

    - Approximate time lines necessary for each activity to complete its part of the COA.

    - Request that members: 1) Staff proposals in their sections; 2) Secure their principal's approval/disapproval; and 3) Report back on Section ability to take the considered action (time: to be announced (TBA) based on time line).

    - Recap of new due outs.

- **Agenda**. An agenda must be used, it must be published in a read-ahead packet, and the agenda's topics should remain relatively constant.

- **Read-ahead packet**. The purpose of the read-ahead packet is to recommend an agenda for the next IOWG meeting and to recommend those IOWG members whose attendance is necessary. All IOWG members are welcome to attend every meeting. It is more efficient to let the meeting agenda dictate who should attend each meeting. One of the most important effects this technique creates is that IOWG members are more likely to attend meetings on a regular basis since they know their time will not be wasted when they do attend. At battalion level, the read-ahead packet may not be necessary due to the small size of the IOWG.

- **Moderator/Noncommissioned officer in charge (NCOIC)**. The moderator must be someone with excellent time management skills who can keep the group on task and on schedule. He must be polite, yet firm. The moderator performs the function of time keeper and note taker. He also assembles and disseminates the read ahead packet. This allows the IOCOORD/officer to run the IOWG without being the drill sergeant. Several units have found that NCOs make the best moderators.

- **Time limit.** IOWG meetings should only long enough to accomplish goals listed in the agenda. Issues that require additional time should be handled in break-out sessions. Once the moderator identifies an issue that requires more time than the agenda calls for, he schedules a break out session with specific IOWG members. This ensures that only those members involved are required to invest their time on any given topic. Meetings lasting longer than 60 minutes create challenges to team building and focus.

- **Due Outs**. Attendees must leave the meeting knowing what their due outs are. Follow up IOWG meetings with a memo to the XO and S-3 if IO team members were not present.

4. MOE

- MOE are a prerequisite to the performance of combat assessment. (JP 1-02). Subjective indicators that the outcomes of tactical actions have achieved or contributed to achieving the desired effect. MOE articulate where to look and what to measure in order to determine if the desired effect has been achieved.

- Combat assessment is the determination of the overall effectiveness of force employment during military operations. Combat assessment is composed of three major components:

    - Battle damage assessment

    - Munitions effectiveness assessment

    - Re-attack recommendation

- MOE characteristics:

    - Focused on assessing the achievement of the objective.

    - Measurable and observable: quantitative values or qualitative descriptions.

    - Timely/responsive: Collection and analysis is rapid enough to support timely decision-making.

    - Cost effective

- How to develop IO MOE

    - **Step 1: Develop the MOE statement.** Use the objective's target, effect, and purpose as a guide to determine what must be observed, reported, and assessed.

    - **Step 2: Develop the leading indicators that support the MOE statement.** Leading indicators are quantifiable signs that measure trends or progress towards attaining the objective. The IO planner should wargame potential leading indicators that will assist in measuring achievement of the IO objective. This is normally done in conjunction with the intelligence representative to the IO cell and other members of the IOWG. The purpose of developing indicators is to:

    - ∗ Establish a baseline of activity from which success or lack of progress can be measured. All indicators should have a baseline of activity from which to measure progress.

    - ∗ Assist the intelligence representative in determining intelligence collection requirements.

    - ∗ Focus the other members of the staff and the components to potential collection requirements.

  - º **Step 3: The IO cell's job is to make known the intelligence requirements and establish a mechanism for tracking progress on accomplishing the objectives.**

    Example:

    Statement: Leadership is influenced to not attack relief operations personnel.

    Indicators:

    - ∗ Decrease in the number of kidnapings or attempted kidnapings of disaster relief personnel.

    - ∗ Decrease in the number of attacks on U.S. military personnel.

    - ∗ Leadership changes rhetoric in open press.

    - ∗ Leadership increases contact with third party envoy.

    - ∗ Intercepts of leadership communications directing no aggression

  - º **Step 4: Coordinate with the intelligence representative on collection requirements related to MOE and indicators.**

  - º **Step 5: Examine the adversary and friendly force structures and determine where to focus IO efforts to achieve the IO objectives.** This analysis should lead to developing critical capabilities and critical requirements that are most vulnerable to IO capabilities.

  - º **Step 6: Determine what effect you want to have on the most critical and vulnerable functions and select the IO capability or capabilities that can best achieve that effect.**

    - ∗ Analyze the initial force structure to determine if the apportioned forces roughly possess adequate IO capabilities.

    - ∗ Identify any shortfalls and request additional resources from higher.

- Potential MOE. MOE in CMO could include the following:

  - º Drops in mortality rates in the population below a specified level per day.

  - º Increase in water available per day to various levels established for human consumption, to support sanitation measures, and for livestock consumption.

  - º Increase of available electricity.

  - º Increase in the presence and capabilities of NGOs and international organizations.

  - º Increase in oil /gas refinery capacity.

- The last prerequisite for success entails establishing and monitoring MOE for CMO that are useful at strategic, operational, and tactical levels. When looking at MOE for CMO, determine what the standard was before arrival and consider this the baseline that must be improved upon.

Appendix A

Glossary

Part I: Abbreviations and Acronyms

ABE	assistant brigade engineer
AOR	area of responsibility
BCT	brigade combat team
BDA	battle damage assessment
BDE	brigade
C2	command and control
C2W	command and control warfare
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
C4ISR	command, control, communications, computers, intelligence, and reconnaissance
CA	civil affairs
CATA	civil affairs team alpha
CATB	civil affairs team bravo
CENTCOM	Central Command
CI	counterintelligence
CMA	civil military assistance
CMO	civil military operations
CNA	computer network attack
COA	course of action
COE	common operating environment

COG	center of gravity
COMCAM	combat camera
COMPUSEC	computer security
CP	command post
CREG	communications, religion, economy governance
CS	combat support
CSS	combat service support
DOD	Department of Defense
DTG	date/time group
ECC	effects coordination cell
EEFI	essential elements of friendly information
ENCOORD	engineer coordinator
ENG	engineer
EP	electronic protection
ETO	effects tasking order
EW	electronic warfare
FECC	fires and effects coordination cell
FIST	fires support team
FSE	fire support element
FSO	fire support officer
GLOC	ground lines of communication
HA	humanitarian assistance
HDR	humanitarian daily ration
HEP	hepatitis

HN	host nation
HUMINT	human intelligence
IM	information management
INFOSEC	information security
IO	information operations
IOWG	information operations working group
IPB	intelligence preparation of the battlefield
IP	Iraqi police
ISF	Iraqi security forces
ISO	in support of
ISR	intelligence, surveillance, and reconnaissance
IW	information warfare
JTF	joint task force
JRTC	Joint Readiness Training Center
LN	local nation/nationals
LNO	liaison officer
MCO	major combat operations
MDMP	military decision-making process
MEDCAP	medical civil action/affairs program
MEDEVAC	medical evacuation
METL	mission essential task list
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MOE	measures of effectiveness

MRE	mission readiness/rehearsal exercises
NBC	nuclear, biological, and chemical
NETOPS	net operations
NGO	nongovernmental organization
Obj	objective
O©	observer controller
OPFOR	opposing force
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security
PAO	public affairs officer
PCC	project coordination cell
PIR	priority intelligence requirements
PA	public affairs
PMCO	post major combat operations
PMO	provost marshal officer
POC	point of contact
PSYOP	psychological operations
RCP	radar communication processor
RISTA	reconnaissance, surveillance, and target acquisition
RM	resource manager
ROMO	range of military operations
SA	situational awareness
SIO	special information operations

SIR	specific information requirement
SITEMP	situation template
SJA	staff judge advocate
SOF	special operations forces
SOPs	standing operating procedures
SOR	specific operational requirement
SWEAT-MS	sewage, water, energy, academics, trash medical, security
TB	tuberculosis
TBA	to be announced
TCP	traffic control points
TF	task force
TOC	tactical operations center
TPD	tactical PSYOP detachment
TPT	tactical PSYOP team
TTP	tactics, techniques, and procedures
UBL	unit basic load
XO	executive officer

Part II: Terms and Definitions

A. Terms

Civil Affairs. The activities of a commander that establishes, maintains, influences, or exploits relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Joint Pub 1-02

Command and Control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Joint Pub 1-02

Communications Security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications security includes a. Crypto security and physical security - The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. Transmission security - The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. Emission security - The component of communications that results from all measures taken to deny unauthorized persons information f value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. Physical security - The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observations thereof by unauthorized persons. Joint Pub 1-02

Computer Network Attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Joint Pub 1-02

Computer Security. The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems; also called COMPUSEC. Joint Pub 1-02

Counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. Joint Pub 1-02

Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assignations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. Joint Pub 1-02

Deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interested. Joint Pub 1-02

Defense Information Infrastructure. The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DoD local, national, and worldwide information needs. The Defense Information Infrastructure connects DoD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence and commercial communications systems used to transmit DoD information. Also called DII. Joint Pub 1-02

Defense Information Operations. Integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted though information assurance, physical security, operations security, counterdeception, counterpsychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Joint Pub 1-02

Incident. In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing, disruption, or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. Joint Pub 1-02

Indications and Warning. Those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that could involve a threat to the United States or allied/coalition military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the U.S., its overseas forces, or allied/coalition nations; hostile reactions to U.S. reconnaissance activities, terrorists' attacks; and other similar events. Also called I&W. Joint Pub 1-02

Information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. Joint Pub 1-02

Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporation protection, detection, and reaction capabilities. Also call IA. Joint Pub 1-02

Information-Based Process. Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or system of systems or processes. Joint Pub 1-02

Information Environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. Joint Pub 1-02

Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. Joint Pub 1-02

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

Information Superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Joint Pub 1-02

Information System. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. Joint Pub 1-02

Information Warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW. Joint Pub 1-02

Intelligence Preparation of the Battlefield. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battle space builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation for the battle space is a continuous process. Also called IPB. Joint Pub 1-02

Leveraging. In information operations, the effective use of information, information systems, and technology to increase the means and synergy in accomplishing information operations strategy. Joint Pub 1-02

Military Deception. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions or inactions that will contribute to the accomplishment of the friendly mission. The five categories of military deception: 1. Strategic military deception - military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator strategic military objectives, policies, and operations. 2. Operations military deception - military deception planned and executed by and in support of operations-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations. 3. Tactical military deception - military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. 4. Service military deception - military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems. 5. Military deception in support of operations security OPSEC - military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities. Joint Pub 1-02

Offensive Information Operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisions makers to achieve or promote soporific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack. Joint Pub 1-02

Operations Security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: 1. Identify those actions that can be observed by adversary intelligence systems. 2. Determine indicators hostile intelligence systems might obtain that could be interoperated or pieced together to derive critical information in time to be useful to adversaries. 3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. Joint Pub 1-02

Perception Management. Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning, and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting from foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. Joint Pub 1-02

Physical Security. The part of security concerned with physical measures, designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. Joint Pub 1-02

Probe. In information operations, any attempt to gather information about an automated information system or its on-line users. Joint Pub 1-02

Physical Operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations s to induce or reinforce foreign attitudes and behaviors favorable to the originator's objective. Also called PSYOP. Joint pub 1-02

Public Affairs. Those public information, command information, and community relations activities directed toward both the external and internal public with interest in the Department of Defense. Also called PA. Joint Pub 1-02

Special Information Operations. Information operations that by their sensitive nature, due to their potential effect or impact, security requirement, or risk to the national security of the United States, require a special review and approval process. Also called SIO. Joint Pub 1-02

Vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system which cause it to suffer a definite degradation incapability to perform the designated mission as a result of having been subjected to a certain level of effects in an unnatural manmade hostile environment. 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. Joint Pub 1-02

Vulnerability Analysis. In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness or proposed security measures, and confirm the adequacy of such measures after implementation. Joint Pub 1-02

B. Definitions

Defensive IO - integrates and coordinates policies, procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO is conducted through information assurance, OPSEC, physical security, counterdeception, counterpropaganda, counterintelligence, EW, and SIO. Defensive IO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Defensive IO ensures the necessary protection and defense of information and information systems upon which forces depend to conduct operations and achieve mission objectives. Four interrelated process support defensive IO -- information environment protection, attack detection, capability restoration, and attack response. Because they are interrelated, full integration of offensive and defensive IO is essential.

Information - Facts, data, or instructions in any medium or form. It is the meaning that a human assigns to do by means of the known conventions used in their representations. The same information may convey different messages to different receipts and thereby provide mixed signals to information gathers and users to include the intelligence community.

Information Assurance - IO that protects and defends information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiations. This includes providing for restoration for information systems by incorporating protection, detection, and reaction capabilities.

Information-Based Process - processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand alone processes or sub-processes which, taken together, comprise a larger system or systems or processes. At the tactical level, information- based processes include reconnaissance plans, decision making, and local traffic control points in austere areas.

Information Environment - the aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself.

Information Operations - actions taken to affect adversary information and information systems while defending one's own information and information systems. IO requires close, continuous integration of offensive and defensive capabilities and activities, as well as the effective design, integration, and interaction of C2 with intelligence support. Major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include CNA. IO-related activities include, but are not limited to, PA and CA.

Information Superiority - the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority may be all pervasive in the AOR or it may be function-aspect-specific, localized, and temporal.

Information System - the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. The information system also includes the information- based processes.

Information Warfare - information operations conducted during a time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Offensive IO - OPSEC, military deception, PSYOP, electronic warfare, physical attack, destruction, and computer attack. Offensive IO can be conducted in a variety of situations and circumstances across the range of military operations. Offensive IO may have the greatest impact prior to open hostilities, but applies to all levels of war.

IO Organization

Unit commanders should establish a fully functioning IO cell to develop and promulgate guidance/plans for IO that are passed to subordinate units for decentralized planning and execution. The IO cell integrates a broad range of potential actions and activities that help contribute to the commander's desired end state in the area of responsibility. The commander's cell must be structured to plan and coordinate IO and sufficiently flexible to accommodate a variety of planning and tactical circumstances. All principal staff must be an active part of IO planning.

IO Planning

IO planning is accomplished in MDMP. IO planning must be broad based and encompass employment of all available capabilities. IO planning must analyze the risk of compromise, reprisal, escalation of hostilities, and insubordination or inadvertent counteraction of IO.

Appendix B

IO Planner's Aid

Key Definitions

Information Operations: The employment of the core capabilities of EW, CNO, PSYOP, military deception, and OPSEC, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decsionmaking. (FM 3-13)

Information Environment: The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (FM 3-0)

Information Superiority: The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (FM 3-0)

Field Support Division May 2004

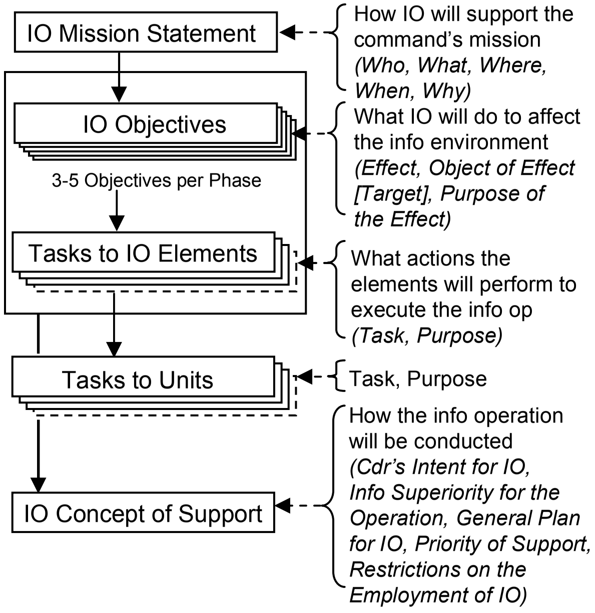
IO and MDMP

MDMP Step	IO Focus
Receipt of Mission	• Conduct initial assessment of info op • Determine IO planning requirements
Mission Analysis	• Understand IO situation • Analyze HHQ information operation • Define & analyze the info environment and threat • Develop IO mission statement & objectives • Seek commander's IO guidance
COA Development	• ID friendly IO capabilities & vulnerabilities • Develop IO concept of support
COA Analysis	• Visualize operations in the info environment • Wargame IO concept of support against how the enemy will employ its information systems and assets
COA Comparison	• Analyze & evaluate IO support to each COA
COA Approval	• Finalize details of the information operation
Orders Production	• Prepare IO annex & input to base order/plan

IO Integration with IPB

IPB Step	IO Focus	Analysis Product
Define the Battlefield	Define the Information Environment	Combined Information Overlay - Significant characteristics of the info environment & effects on operations
Describe the Battlefield's Effects	Describe the Information Environment's Effects	
Evaluate the Threat	Evaluate the Threats' Info System	Threat COG Analysis - Critical vulnerabilities Threat Templates - Who makes decisions; what nodes, links, & systems the threat uses; how info assets are employed
Determine Threat COAs	Determine Threat Actions in the Info Environment	Information SITEMP - When, where, & why the threat will seek to gain info superiority

Mission to Task Products



How IO will support the command's mission *(Who, What, Where, When, Why)*

What IO will do to affect the info environment *(Effect, Object of Effect [Target], Purpose of the Effect)*

What actions the elements will perform to execute the info op *(Task, Purpose)*

Task, Purpose

How the info operation will be conducted *(Cdr's Intent for IO, Info Superiority for the Operation, General Plan for IO, Priority of Support, Restrictions on the Employment of IO)*

Example IO Mission and Objectives

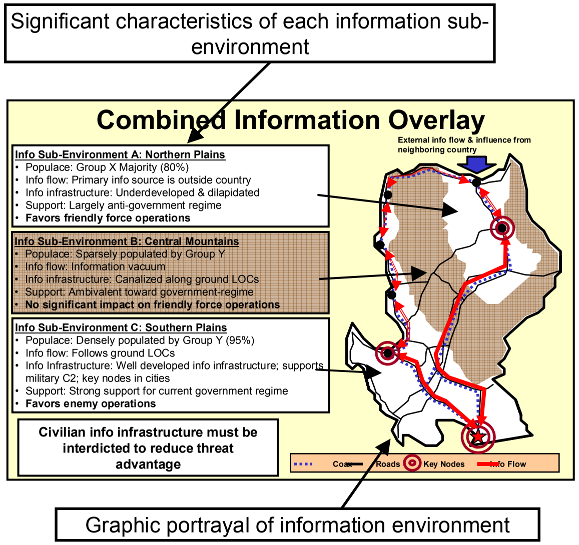
(Tactical Corps mission)

IO Mission: On order, XX Corps IO disrupts 1st Operational Strategic Command (OSC) ground and air defense forces' command and control, influences civilian populace perceptions, and protects Corps' critical information in the AOR in order to facilitate destruction of 1st OSC forces.

IO Objectives:

- Disrupt 1st OSC AD C2 in order to prevent coordinated engagement of XX Corps' deep attacks.
- Destroy 1st OSC headquarters in order to neutralize command and control between battlezone and reserve forces.
- Disrupt operational reserve CPs and communication nets in order to delay employment of reinforcing or counterattack forces.
- Influence civilian populace in occupied areas in order to minimize interference with XX Corps' operations.
- Deny SPF detection and identification of XX Corps' main and tactical CPs in order to prevent targeting by 1st OSC artillery fires.

Example Combined Information Overlay


Significant characteristics of each information sub-environment

Combined Information Overlay

Info Sub-Environment A: Northern Plains
- Populace: Group X Majority (80%)
- Info flow: Primary info source is outside country
- Info infrastructure: Underdeveloped & dilapidated
- Support: Largely anti-government regime
- **Favors friendly force operations**

Info Sub-Environment B: Central Mountains
- Populace: Sparsely populated by Group Y
- Info flow: Information vacuum
- Info infrastructure: Canalized along ground LOCs
- Support: Ambivalent toward government-regime
- **No significant impact on friendly force operations**

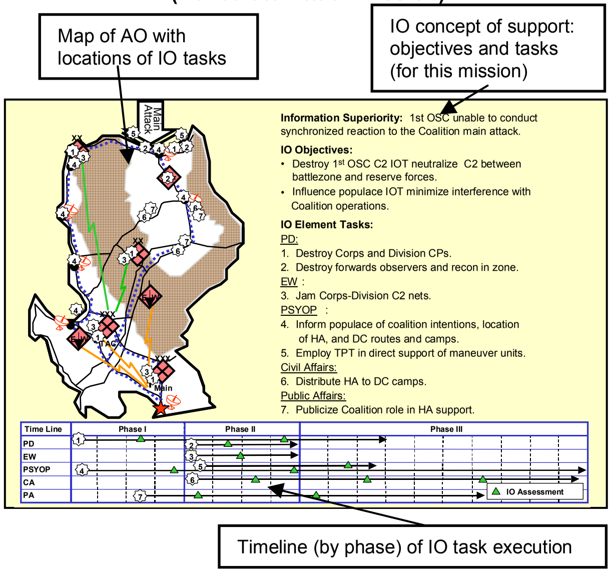
Info Sub-Environment C: Southern Plains
- Populace: Densely populated by Group Y (95%)
- Info flow: Follows ground LOCs
- Info Infrastructure: Well developed info infrastructure; supports military C2; key nodes in cities
- Support: Strong support for current government regime
- **Favors enemy operations**

Civilian info infrastructure must be interdicted to reduce threat advantage

Graphic portrayal of information environment

Example Course of Action Sketch

(Deliberate Attack Mission)


Map of AO with locations of IO tasks
IO concept of support: objectives and tasks (for this mission)
Main Attack
TAC
Main
Time Line
Phase I
Phase II
Phase III
PD
EW
PSYOP
CA
PA
IO Assessment
Timeline (by phase) of IO task execution

Information Superiority: 1st OSC unable to conduct synchronized reaction to the Coalition main attack.

IO Objectives:

- Destroy 1st OSC C2 IOT neutralize C2 between battlezone and reserve forces.
- Influence populace IOT minimize interference with Coalition operations.

IO Element Tasks:

PD:

1. Destroy Corps and Division CPs.
2. Destroy forwards observers and recon in zone.

EW :

3. Jam Corps-Division C2 nets.

PSYOP :

4. Inform populace of coalition intentions, location of HA, and DC routes and camps.
5. Employ TPT in direct support of maneuver units.

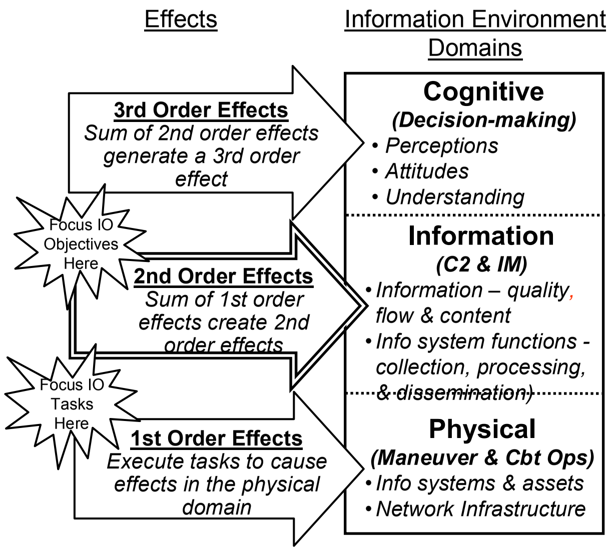
Civil Affairs:

6. Distribute HA to DC camps.

Public Affairs:

7. Publicize Coalition role in HA support.

Generating Effects


Effects
Information Environment Domains
3rd Order Effects
Sum of 2nd order effects generate a 3rd order effect
Focus IO Objectives Here
2nd Order Effects
Sum of 1st order effects create 2nd order effects
Focus IO Tasks Here
1st Order Effects
Execute tasks to cause effects in the physical domain
Cognitive
(Decision-making)
• Perceptions
• Attitudes
• Understanding
Information
(C2 & IM)
• Information – quality, flow & content
• Info system functions - collection, processing, & dissemination)
Physical
(Maneuver & Cbt Ops)
• Info systems & assets
• Network Infrastructure

Doctrinal Effects For IO (FM 3-13)

Destroy – Damage a combat system so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.

Disrupt – In information operations, means breaking or interrupting the flow of information between selected C2 nodes.

Degrade – In information operations, is using non-lethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems, and information collection efforts or means.

Deny – In information operations, entails withholding information about Army force capabilities and intentions that adversaries need for effective and timely decisionmaking.

Deceive – Cause a person to believe what is not true.

Exploit – In information operations, is to gain access to adversary command and control systems to collect information or to plant false or misleading information.

Influence – Cause adversaries or others to behave in a manner favorable to Army forces.

Planning Fires and Effects for IO

MDMP	Targeting Action	IO Action
Mission Analysis	• Determine specified, implied, & essential fire support tasks • Determine HVTL • Translate fire support assets into capabilities • Develop draft targeting objectives or EFSTs	• Nominate targets to HVTL • Determine supporting IO capabilities • Develop IO objectives or EIOTs
COA Dev.	• Develop Concept of Fires (or Effects) • Develop initial HPTL • Quantify effects for EFSTs	• Input to Concept of Fires (or Effects) • Nominate targets to HPTL
COA Analysis & Comp.	• Finalize Concept of Fires • Finalize HPTL • Develop TSM • Develop fire support control measures	• Input to TSM
COA Approval	• Brief fire support plan as part of each COA	• None
Orders Prod.	• Write fires paragraph of & fire support annex	• Cross-walk IO & fire spt annexes

Assessment

This product produced by U.S. Army, 1st Information Operations Command (Land)

Modified IO Annex Format

1. SITUATION.

a. Area of Operations. Describe the info environment.

b. Enemy Operations in the Info Environment. Describe enemy's decision-making structure; C4ISR assets, systems, and functions, assets and organizations available to affect the information environment and friendly C4ISR; and critical capabilities & vulnerabilities.

c. Friendly Cap. & Vulnerabilities in the Info Environment.

d. Civil Considerations.

e. Attachments and Detachments. List organic and supporting assets available to execute the info operation.

2. MISSION. State the IO mission.

3. EXECUTION.

a. Concept of Support. Define info superiority and explain how IO will help achieve it. Describe the info operation (i.e., how IO will be conducted and who will perform it) from beginning to end; to include enemy capabilities & vulnerabilities to be attacked and friendly critical vulnerabilities to be protected.

b. Assessment.

b. Tasks to Subordinate Units.

c. IO Cell. List instructions not listed in the SOP.

d. Coordinating Instructions.

4. SERVICE SUPPORT.

5. COMMAND AND SIGNAL.

Appendix C

IO Integration with IPB

Key References

JP 2-01.3, *Joint TTP for Intelligence Preparation of the Battlespace* (MAY 00)

FM 34-130, *Intelligence Preparation of the Battlefield* (JUL 94)

1st IO CMD (Land) Information IPB TTB (Draft)

IPB Steps

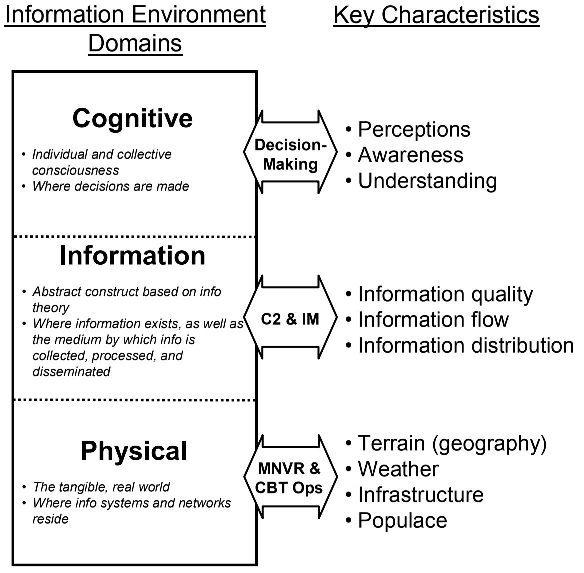
1. Define the Battlefield Environment
2. Describe the Battlefield's Effects
3. Evaluate the Threat
4. Determine Threat Courses of Action (COAs)

Field Support Division October 2002

IO Integration with IPB

IPB Step	IO Focus	Analysis Product
1 Define the Battlefield	Define the Information Environment	Combined Information Overlay - Significant characteristics of the info environment & effects on operations
2 Describe the Battlefield's Effects	Describe the Information Environment's Effects	
3 Evaluate the Threat	Evaluate the Threats' Info System	Threat COG Analysis - Critical vulnerabilities Threat Templates - Who makes decisions; what nodes, links, & systems the threat uses; how info assets are employed
4 Determine Threat COAs	Determine Threat Actions in the Info Environment	Information SITEMP - When, where, & why the threat will seek to gain info superiority

Information Environment Construct



1 Define the Information Environment

Examine the AO to identify significant characteristics of each info environment domain.

Analyze:

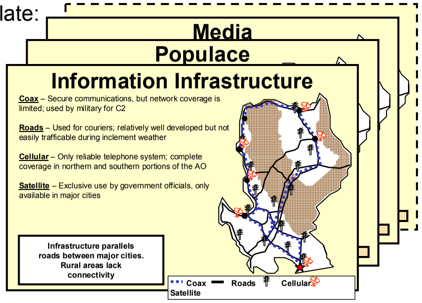
- Terrain – canalization and compartmentalization
- Population demographics – distribution, language, religion, ethnicity, education
- Societal structures and organizations – political, government, religious, paramilitary, criminal
- Civilian information infrastructure – key links and nodes
- Media – radio, TV, print, internet, including audience & users
- Third party organizations – non-government and private
- Information – key ideologies, perceptions and beliefs that may cause specific friendly, threat or third party behavior

Determine:

- Physical Domain – What aspects of the terrain, weather, infrastructure, and populace will impact the employment of information system assets and the linking of information systems into networks?
- Information Domain – What information and its quality, flow, and distribution will impact information systems' functions (i.e., the collection, processing, and dissemination of information)?
- Cognitive Domain – What populace perceptions, attitude, awareness, understanding, and knowledge will influence decision-making?

2 Describe the Information Environment's Effects

1. Analyze each domain's significant characteristics in detail and template:



Coax – Secure communications, but network coverage is limited; used by military for C2

Roads – Used for couriers; relatively well developed but not easily trafficable during inclement weather

Cellular – Only reliable telephone system; complete coverage in northern and southern portions of the AO

Satellite – Exclusive use by government officials, only available in major cities

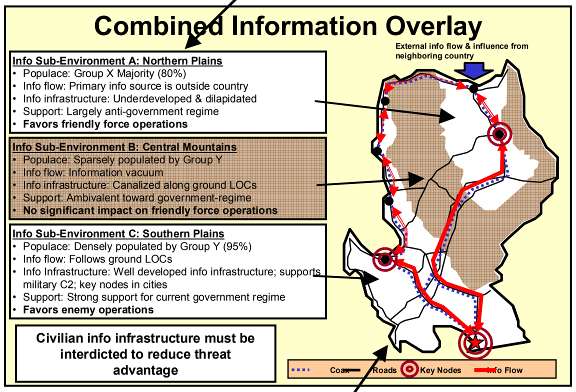
Infrastructure parallels roads between major cities. Rural areas lack connectivity

2. Combine the significant characteristics of the domains to develop aggregate effects for the entire info environment.
3. Plot analysis to create a Combined Information Overlay (CIO). The CIO depicts *where* and *how* the information environment's potential effects will impact military operations. Considerations:
   - Can the AO be divided into distinct sub-information environments?
   - How does information flow in the AO?
   - Is there key terrain in the information environment?

Example CIO

CIO – The "MCOO of the Information Environment"

Significant characteristics of each information sub-environment


Combined Information Overlay
External info flow & influence from neighboring country
Coax
Roads
Key Nodes
Info Flow

Info Sub-Environment A: Northern Plains
- Populace: Group X Majority (80%)
- Info flow: Primary info source is outside country
- Info infrastructure: Underdeveloped & dilapidated
- Support: Largely anti-government regime
- **Favors friendly force operations**

Info Sub-Environment B: Central Mountains
- Populace: Sparsely populated by Group Y
- Info flow: Information vacuum
- Info infrastructure: Canalized along ground LOCs
- Support: Ambivalent toward government-regime
- **No significant impact on friendly force operations**

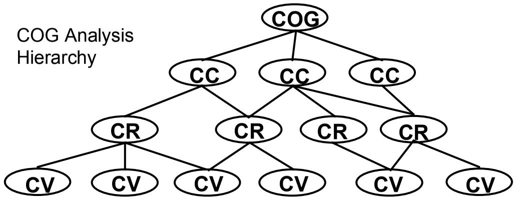
Info Sub-Environment C: Southern Plains
- Populace: Densely populated by Group Y (95%)
- Info flow: Follows ground LOCs
- Info Infrastructure: Well developed info infrastructure; supports military C2; key nodes in cities
- Support: Strong support for current government regime
- **Favors enemy operations**

Civilian info infrastructure must be interdicted to reduce threat advantage

Graphic portrayal of information environment

3 Evaluate the Threat - Centers of Gravity

COG Analysis Hierarchy



Definitions

Center of Gravity (COG): Primary source of moral or physical strength, power, and resistance.

Critical Capability (CC): Primary abilities which merit a COG to be identified as such in the context of a given scenario, situation, or mission.

Critical Requirement (CR): Essential conditions, resources, and means for a critical capability to be fully operative.

Critical Vulnerability (CV): Critical requirements (or components thereof) which are deficient or vulnerable to attack or influence in a manner achieving decisive results.

COG Analysis Steps

1. Identify potential threat COGs. Visualize the threat as a system of functional components. Based upon how the threat organizes, fights, makes decisions, and its physical and psychological strengths and weaknesses, select the threat's primary source of moral or physical strength, power, and resistance.
2. Identify Critical Capabilities (CC). Each COG is analyzed to determine what primary abilities (functions) the threat possesses in the context of the battlefield and friendly mission that can prevent friendly forces from accomplishing the mission. Each identified CC must relate to the COG, otherwise it is not critical in the context of the analysis.
3. Identify Critical Requirements (CRs) for each CC. A CR is a condition, resource, or means that enables threat functions or mission. CRs are usually tangible elements such as communications means, weapons systems, or even geographical areas or features. There may be more than one CR per CC.
4. Identify Critical Vulnerabilities (CVs) for each CR. A CV is a CR, or component of a CR, which is vulnerable to attack or influence. As the hierarchy of CRs, and CVs are developed, inter-relationships and overlapping between the factors are sought in order to identify CRs and CVs that support more than one CC. When selecting CVs, CV analysis is conducted to pair CVs against friendly capabilities.

Validity Testing for COGs

✓ Will destruction, neutralization, or substantial weakening of the COG result in changing the threat's COA or denying its objective?

✓ Does the friendly force have the resources and capability to accomplish destruction or neutralization of the threat COG? If the answer is "no", then the threat's identified critical factors must be reviewed for other critical vulnerabilities, or planners must reassess how to attack the previously identified critical vulnerabilities with additional resources.

Criteria for CV Analysis (CARVER)

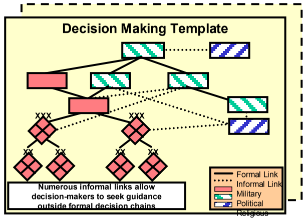
- **C**riticality. An estimate of the CVs importance to the enemy. A vulnerability will significantly influence the enemy's ability to conduct or support operations.
- **A**ccessibility. A determination of whether the CV is accessible to the friendly force in time and place.
- **R**ecuperability. An evaluation of how much effort, time, & resources the enemy must expend if the CV is successfully affected.
- **V**ulnerability. A determination of whether the friendly force has the means or capability to affect the CV.
- **E**ffect. A determination of the extent of the effect achieved if the CV is successfully exploited.
- **R**ecognizability. A determination if the CV, once selected for exploitation, can be identified during the operation by the friendly force, and can be assessed for the impact of the exploitation.

3 Evaluate the Threat - Templating

Model the threat by producing templates that portray the normal or doctrinal (historical) composition and organization of the adversary's information system and its assets.

The result should identify adversary capabilities and vulnerabilities under ideal conditions in the information environment.

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

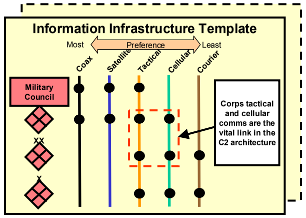

Decision Making Template
XXX
XX
XX
XXX
XX
XX
Numerous informal links allow decision-makers to seek guidance outside formal decision chains
Formal Link
Informal Link
Military
Political
Religious

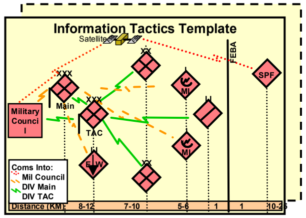
Decision-Making Template – *Who* in an organization makes decisions. Purpose is to determine how an adversary organization operates to achieve its mission or goals. Consider:
- Structure of the organization
- Critical linkages & inter-relationships
- Key decision makers
- Decision-making characteristics (i.e. centralized, decentralized, other)

This product produced by U.S. Army, 1st Information Operations Command (Land)

Templating (continued)

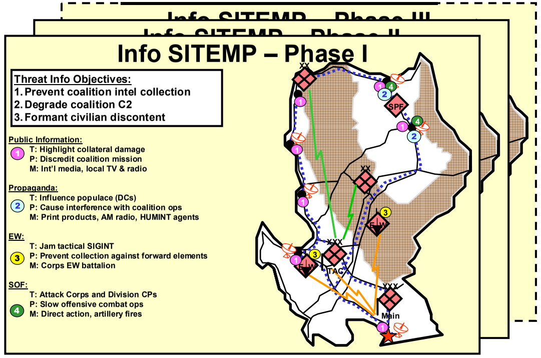
Information Infrastructure Template
What nodes, links, assets, and means an organization uses to collect, process, & disseminate information. Purpose is to identify critical adversary information system nodes, links, & systems (to include those assets capable of impacting the information environment).
Consider:
- Information nodes and links
- Communications means
- Support systems


Information Infrastructure Template
Most
Preference
Least
Coax
Satellite
Tactical
Cellular
Courier
Military Council
XX
Corps tactical and cellular comms are the vital link in the C2 architecture



Information Tactics Template
How the adversary will employ available information assets. Purpose is to identify adversary information and information system capabilities, vulnerabilities, and susceptibilities. Consider:
- Doctrine
- Information-capable assets
- Employment of information assets

4 Determine Threat Activities in the Information Environment


Info SITEMP – Phase III
Info SITEMP – Phase II
Info SITEMP – Phase I
Threat Info Objectives:
1. Prevent coalition intel collection
2. Degrade coalition C2
3. Formant civilian discontent
Public Information:
1 T: Highlight collateral damage
P: Discredit coalition mission
M: Int'l media, local TV & radio
Propaganda:
2 T: Influence populace (DCs)
P: Cause interference with coalition ops
M: Print products, AM radio, HUMINT agents
EW:
3 T: Jam tactical SIGINT
P: Prevent collection against forward elements
M: Corps EW battalion
SOF:
4 T: Attack Corps and Division CPs
P: Slow offensive combat ops
M: Direct action, artillery fires
SPF
XX
XXX
TAC
Main
EW

Information SITEMP – *Where, When, & Why* the threat will employ its information systems. Result is an overall concept and supporting objectives that describes how the adversary will operate in the information environment.
- Why – Likely information concept & objectives and task & purpose of primary information assets
- Where – Location of primary information assets
- When – Prediction of when in the operation info assets will be employed

Threat

COG Analysis Aid

Key References

JP 5-00.1, *Joint Doctrine for Campaign Planning* (Jan 2002)

FM 3-0, *Operations* (Jun 2001)

FM 34-36, *SOF Intelligence and EW Operations* (Sep 1991)

1st IO CMD Information IPB TTP (Draft)

Key Definitions

Center of Gravity (COG): Characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight. (JP 5-00.1)

Critical Capability (CC): Capabilities that are considered crucial enablers for the ***adversary's*** COG to function as such, and are essential to the accomplishment of the adversary's assumed objective(s). (JP 5-00.1)

Critical Requirement (CR): Essential conditions, resources, and means for a critical capability to be fully operational. (JP 5-00.1)

Critical Vulnerability (CV): Aspects or components of the ***adversary's*** critical capabilities (or components thereof), which are deficient or vulnerable to neutralization, interdiction, or attack in a manner achieving decisive or significant results. (JP 5-00.1)

Field Support Division

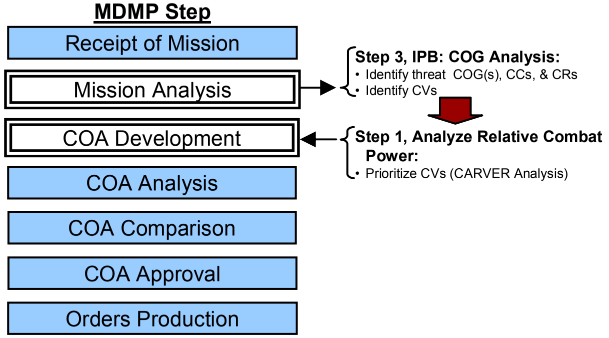
December 2002

Threat COG Analysis and the MDMP

The purpose of performing a threat COG analysis is to determine and evaluate the enemy's (and others') critical vulnerabilities for exploitation.

Since this tool is used to evaluate the threat, the appropriate time to perform this analysis is during Step 3 (Evaluate the Threat) of IPB. The results of COG analysis are later used during COA Development to exploit identified vulnerabilities.

COG analysis of the threat should be conducted by the G2. The IO staff will provide input to, and use, COG analysis to determine what aspects of the threat IO should engage.



MDMP Step

Receipt of Mission

Mission Analysis

COA Development

COA Analysis

COA Comparison

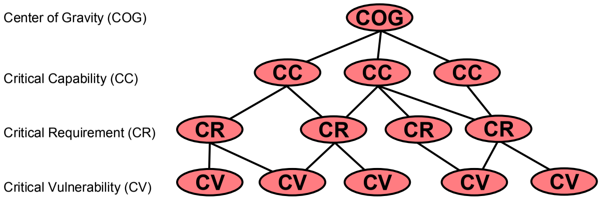
COA Approval

Orders Production

Step 3, IPB: COG Analysis:
- Identify threat COG(s), CCs, & CRs
- Identify CVs

Step 1, Analyze Relative Combat Power:
- Prioritize CVs (CARVER Analysis)

COG Analysis Hierarchy



Center of Gravity (COG). At the strategic level there is usually only one COG. At operational and tactical levels there may be more than one COG. A COG may shift as an operation changes phases.

Critical Capability (CC). Each COG can have multiple critical capabilities in the context of the battlefield and friendly mission.

Critical Requirement (CR). Each CC can have several critical requirements. Critical requirements may be shared by multiple CCs.

Critical Vulnerability (CV). Each CR can have several critical vulnerabilities. Critical vulnerabilities may be shared by multiple CRs.

COG Analysis Steps

1. **Identify Threat Center(s) of Gravity (COG).** Visualize the threat as a system of functional components. Based upon how the threat organizes, fights, makes decisions, and its physical & psychological strengths and weaknesses, select the threat's primary source of moral or physical strength, power, & resistance. *Note: Depending on the level (i.e. strategic, operational, tactical), COGs may be tangible entities or intangible concepts.*

   Validity Testing for COGs:
   - ✓ Will the destruction, neutralization, or substantial weakening of the COG result in changing the threat's COA or denying its objective(s)?

2. **Identify Critical Capabilities (CC).** Each COG is analyzed to determine what primary abilities (functions) the threat possesses in the context of the battlefield and friendly mission that can prevent friendly forces from accomplishing the mission. *Note: CCs are not tangible objects but rather are threat functions.*

   Validity Testing for CCs:
   - ✓ Is the identified critical capability a primary ability in context with the given missions of both threat and friendly forces?
   - ✓ Is the identified CC directly related to the COG?

COG Analysis Steps (continued)

3. **Identify Critical Requirements (CRs).** Each CC is analyzed to determine what conditions, resources, or means that enables threat functions or mission. *Note: CRs are usually tangible elements such as communications means, weapons systems, or even geographical areas or terrain eatures.*

   Validity Testing for CRs:
   - ✓ Will the absence or loss of the identified CR disable the threat's CC?
   - ✓ Does the threat consider the identified CR to be critical (do not mirror image)?

4. **Identify Critical Vulnerabilities (CVs).** Each CC is analyzed to determine which CRs, or components thereof, are vulnerable to neutralization, interdiction, or attack. *Note: CVs may be tangible structures or equipment, or it may be an intangible perception, populace belief or susceptibility.*

   Validity Testing for CVs:
   - ✓ Will exploitation of the CV disable the associated CR?
   - ✓ Does the friendly force have the resources to effect the identified CV?

COG Analysis Steps (continued)

5. **Prioritize CVs.** CARVER is a SOF methodology used to prioritize targets. The methodology can be used to rank-order critical vulnerabilities, thereby prioritizing the targeting process. Apply the six criteria against each CV to determine impact on the threat organization. See Appendix D, FM 34-36 for more information on CARVER.
   - ***C**riticality*. An estimate of the CV's importance to the enemy. To what extent will the vulnerability influence the enemy's ability to conduct or support operations.
   - ***A**ccessibility*. A determination of whether the CV is accessible to the friendly force in time and place. In other words, does the friendly force have the resources and capability to accomplish destruction or neutralization of the CV?
   - ***R**ecuperability*. An evaluation of how much effort, time, & resources the enemy must expend if the CV is successfully affected.
   - ***V**ulnerability*. A determination of whether the friendly force has the means or capability to affect the CV.
   - ***E**ffect*. A determination of the extent of the effect achieved if the CV is successfully exploited.
   - ***R**ecognizability*. A determination if the CV, once selected for exploitation, can be identified during the operation by the friendly force, and can be assessed for the impact of the exploitation.

Friendly

COG Analysis Aid

Key References

JP 5-00.1, *Joint Doctrine for Campaign Planning* (Jan 2002)

FM 3-0, *Operations* (Jun 2001)

FM 34-36, *SOF Intelligence and EW Operations* (Sep 1991)

1st IO CMD COA Development TTP (Draft)

Key Definitions

Center of Gravity (COG): Characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight. (JP 5-00.1)

Critical Capability (CC): Capabilities that are considered crucial enablers for the ***friendly*** COG to function as such, and are essential to the accomplishment of the adversary's assumed objective(s). (mod JP 5-00.1)

Critical Requirement (CR): Essential conditions, resources, and means for a critical capability to be fully operational. (JP 5-00.1)

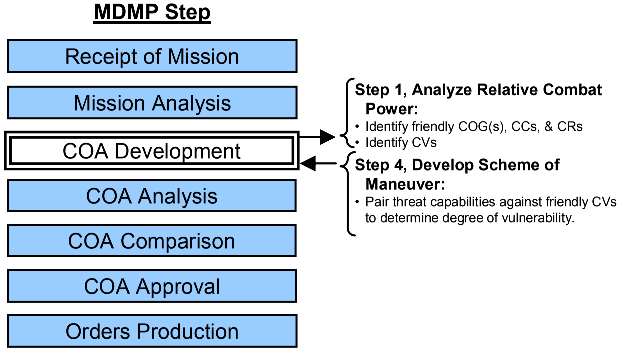
Critical Vulnerability (CV): Aspects or components of the ***friendly*** critical capabilities (or components thereof), which are deficient or vulnerable to neutralization, interdiction, or attack in a manner achieving decisive or significant results. (modified JP 5-00.1)

Field Support Division December 2002

Fitting Friendly COG Analysis into the MDMP

The purpose of performing a friendly COG analysis is to determine and evaluate the friendly force's critical vulnerabilities. Once identified, these vulnerabilities are addressed as a defensive plan within the overall concept of the operation.

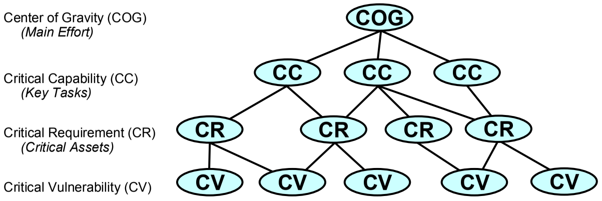
Since this tool is used to identify friendly force vulnerabilities relative to the planned scheme of maneuver, the best time to perform this analysis is during COA Development:



Step 1, Analyze Relative Combat Power:
- Identify friendly COG(s), CCs, & CRs
- Identify CVs

Step 4, Develop Scheme of Maneuver:
- Pair threat capabilities against friendly CVs to determine degree of vulnerability.

COG Analysis Hierarchy



Center of Gravity (COG). The friendly tactical / operational COG is the force designated to execute the main effort. Since the main effort shifts as an operation changes phases, so will the COG.

Critical Capability (CC). Critical capabilities of the friendly COG are those key task(s) that the main effort must accomplish.

Critical Requirement (CR). Each CC can have several critical requirements. Critical requirements may be shared by multiple CCs.

Critical Vulnerability (CV). Each CR can have several critical vulnerabilities. Critical vulnerabilities may be shared by multiple CRs.

COG Analysis Steps

Note: This methodology for analyzing the friendly force is based on the assumption that the friendly force COG is the main effort for the operation. This concept is most valid at the operational and tactical levels.

1. **Identify Friendly Center(s) of Gravity (COG).** Select the friendly force designated to execute the operation's main effort as the COG. If the main effort changes during the operation (i.e. by phase), then so will the COG.

   Validity Testing for COGs:
   - ✓ Will the destruction, neutralization, or substantial weakening of the COG result in changing the friendly COA or denying its objective(s)?

2. **Identify Critical Capabilities (CC).** Select the main effort's key tasks identified by the G3 planner. These tasks become the critical capabilities for that phase of the operation.

   Validity Testing for CCs:
   - ✓ Is this task critical to the success of the main effort in the context of the given mission (task)?
   - ✓ If the COG does not successfully execute the CC, will the COA change?

COG Analysis Steps (continued)

3. **Identify Critical Requirements (CRs).** Each CC (task) needs critical assets in order to execute the task. These critical assets become the critical requirements for that CC.

   Validity Testing for CRs:
   - ✓ Can the COG conduct the CC with the loss of the identified CR?

4. **Identify Critical Vulnerabilities (CVs).** The CRs identified have inherent vulnerabilities as well as vulnerabilities based upon threat capabilities. These identified CVs must be accounted for when developing COAs so reduce the operational risk associated with the mission.

   Validity Testing for CVs:
   - ✓ Will exploitation of the CV disable the associated CR?
   - ✓ Does the threat have the resources to effect the identified CV?
   - ✓ Can the CV be effected by any other entity other than the threat?

This product produced by U.S. Army, 1st Information Operations Command (Land)

COG Analysis Steps (continued)

5. **Prioritize CVs.** The CARVER methodology can be used to rank-order critical vulnerabilities, thereby prioritizing the operations to mitigate these vulnerabilities. See Appendix D, FM 34-36 for more information on CARVER.

   - *Criticality*. An estimate of the CV's importance to the friendly force. To what extent will the vulnerability influence the friendly force's ability to conduct or support operations.
   - *Accessibility*. A determination of whether the CV is accessible to the threat in time and place. In other words, does the threat have the resources and capability to accomplish destruction or neutralization of the CV?
   - *Recuperability*. An evaluation of how much effort, time, & resources the friendly force must expend if the CV is successfully affected.
   - *Vulnerability*. A determination of whether the threat has the means or capability to affect the CV.
   - *Effect*. A determination of the extent of the effect achieved if the CV is successfully exploited.
   - *Recognizability*. A determination if the CV, once selected for exploitation, can be identified during the operation by the threat, and can be assessed for the impact of the exploitation.

Appendix D

Developing an Assessment Plan

1. Develop BDA for key IO tasks.
   - BDA should determine what friendly and adversary actions occurred in the physical and info domains (1st & 2nd order effects).
2. Develop MOE to determine effects in the information and cognitive domains (2nd & 3rd order effects).
   - Write one or more MOE to assess each IO objective.
3. Develop CA to determine results in the cognitive domain (3rd order effects).
   - CA should assess if decision-makers are responding as predicted.
4. Write the assessment plan; include in IO annex.
5. Develop a mechanism to obtain information needed to determine 1st, 2nd, & 3rd order effects:
   - Submit RFIs based upon the assessment plan.
   - Develop IO input to CCIR.
   - Coordinate with BDA reporting with DOCC and targeting board.
   - Review assessments at IOWGs.
   - Monitor intelligence & operations incident reporting.

Assessment Tools

Assessment tools support BDA, MOE, and CA by helping correlate events (i.e., establish cause and effect) in the physical, information, & cognitive domains to IO tasks, objectives, and mission.

Two commonly used assessment tools are:

Trend Analysis – Measures changes in the operating environment. Can be used to:

- Organize observed activities in the information environment in a way that assists the drawing of conclusions.
- Provide indirect indicators (e.g., events / actions not conclusively correlated to the information operation, but may be the result of IO) to support estimation of aggregate IO effects.

Impact Assessment – A PSYOP tool used to determine the effectiveness of an operation by providing indicators of behaviors or attitudes relative to the operation's objectives. Can be used to:

- Provide indicators that objectives are resulting in the desired 2nd and 3rd order effects.
- Determine effectiveness of the information operation.

This product produced by U.S. Army, 1st Information Operations Command (Land)

Example Assessment for an Objective

IO Objective: Disrupt ground force commander's C2 in order to prevent synchronization of corps and division operations.

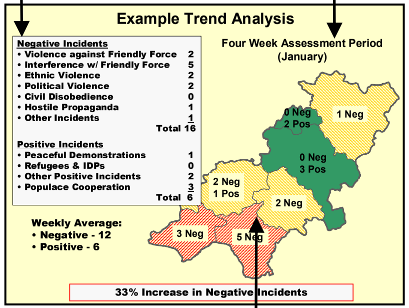
1st Order Effect (BDA) for Physical Domain	2nd Order Effect (BDA/MOE) for Info Domain	3rd Order Effect (MOE/CA) for Cognitive Domain
• Destroyed corps & division HQs. • Destroyed or captured recon, intelligence, surveillance, & target acq (RISTA) assets. • Destroyed or jammed commo nodes. • No attacks against friendly force critical assets.	• Decreased corps & division-level commo traffic. • 1st & 2nd operational groups unable to synchronize fires and maneuver above division level.	Enemy Cdr commits reserve force to the east away from friendly forces' main attack.

Trend Analysis

1. Determine frequency of analysis.
2. Determine what activity / events must be recorded.
3. Establish baseline activity.
4. Measure and analyze magnitude and rates of change to the baseline in terms of time, place, and type of activity.

Activity – Type of activity and number of incidents during the assessment period

Time – Period of assessment during which the incidents occurred



Place – Location in AO where recorded incidents occurred

Assessment Tips

1. Keep the information operation simple, or assessment of 2nd and 3rd order effects may be impossible.
2. Be as objective as possible when assessing BDA. Assessment of the information and cognitive domains will be partially, if not entirely, subjective.
3. Use analysis tools to support conclusions.

- Do not fixate the assessment effort on the physical domain.
- Seek to establish cause and effect in each information environment domain.
- It is necessary to understand IO's aggregate effects in the physical domain in order to draw a valid conclusion about effects in the information and cognitive domains.

Impact Assessment

- Impact indicators are observable behavior that indicate success or failure to achieve the IO objectives.
- Two types of indicators: Positive – Activity that correlates with the objectives' effects. Negative – Activity that is opposite of the the objectives' desired effects.

Example Impact Indicator Analysis

IO Objectives	Indicators	Assessment
Influence populace to support US operations	▼ 3 Violent demonstrations directed against US Forces ▲ Tensions easing between Governor A and US Forces ▲ Political leaders publicly praise US presence and operations	A No Change
Deny insurgent support from local populace	▼ Insurgents paid rewards to kill pro-US government officials ▼ 3 Incidents of insurgent recruiting ▲ Increased populace reporting on insurgent activity	R No Change
Disrupt extremist influence	▲ Hardliner rally poorly attended ▲ Local newspaper denounces extremist leader	G Improvement

IO Assessment Aid

Key Definitions

Battle Damage Assessment (BDA): The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. (JP 1-20)

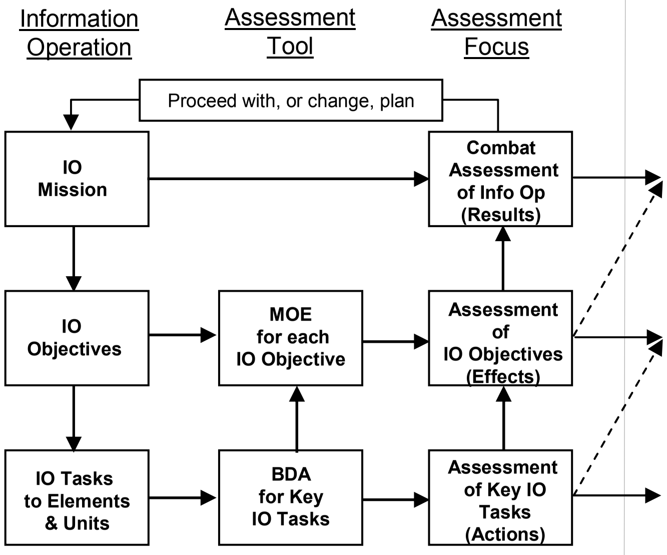
Measures of Effectiveness (MOE): Tools used to measure results achieved in the overall mission and execution of assigned tasks. MOE are a prerequisite to the performance of combat assessment. (JP 3-60)

Combat Assessment (CA): The determination of the overall effectiveness of force employment during military operations. (JP 3-60)

Field Support Division

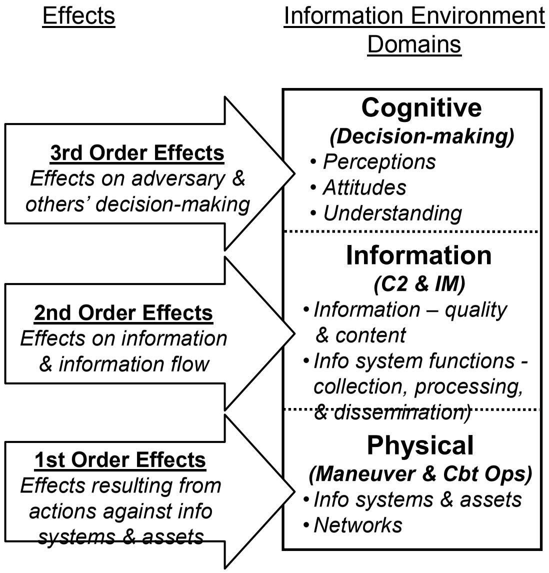
December 2002

Assessment Methodology



Information Operation
Assessment Tool
Assessment Focus
Proceed with, or change, plan
IO Mission
Combat Assessment of Info Op (Results)
IO Objectives
MOE for each IO Objective
Assessment of IO Objectives (Effects)
IO Tasks to Elements & Units
BDA for Key IO Tasks
Assessment of Key IO Tasks (Actions)

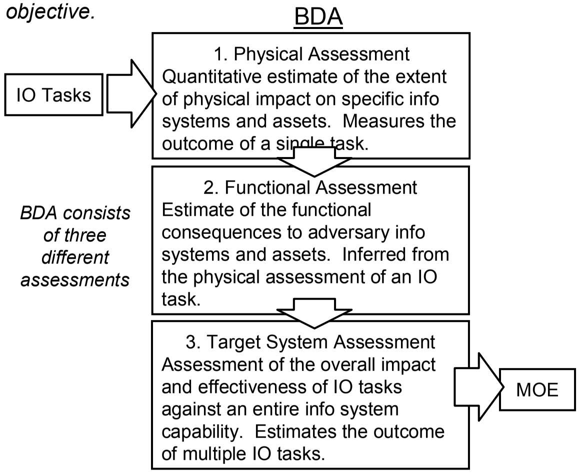
Hierarchy of Effects



Effects
Information Environment Domains
3rd Order Effects
Effects on adversary & others' decision-making
2nd Order Effects
Effects on information & information flow
1st Order Effects
Effects resulting from actions against info systems & assets
Cognitive
(Decision-making)
• Perceptions
• Attitudes
• Understanding
Information
(C2 & IM)
• Information – quality & content
• Info system functions - collection, processing, & dissemination)
Physical
(Maneuver & Cbt Ops)
• Info systems & assets
• Networks

Battle Damage Assessment (BDA)

BDA measures the effects of friendly actions against adversary info systems and assets in the physical domain in order to determine whether IO tasks or sets of tasks have accomplished the intended purpose. As a minimum, key IO tasks should have BDA. *Note: BDA must be objective.*



1. Physical Assessment
Quantitative estimate of the extent of physical impact on specific info systems and assets. Measures the outcome of a single task.

2. Functional Assessment
Estimate of the functional consequences to adversary info systems and assets. Inferred from the physical assessment of an IO task.

3. Target System Assessment
Assessment of the overall impact and effectiveness of IO tasks against an entire info system capability. Estimates the outcome of multiple IO tasks.

Measures of Effectiveness (MOE)

MOE estimate the aggregate effects of IO tasks to determine if the IO objectives are creating the desired effects in the info and cognitive domains.

2nd Order MOE – Estimate effects in the info domain (info quality, content, & flow).

3rd Order MOE – Estimate effects in the cognitive domain (enemy & other ldrs' perceptions, attitudes, & understanding).

Writing MOE:

- Each IO objective should have one or more MOE.
- If possible, MOE should be observable, quantifiable, precise, and correlated to the effect of the objective.
- Use the objective's purpose as a guide to what must be observed, reported, and assessed.
- If an MOE is difficult to write for a particular objective, then re-visit the objective to ensure it has a clearly defined, attainable effect. If necessary, re-write the objective.

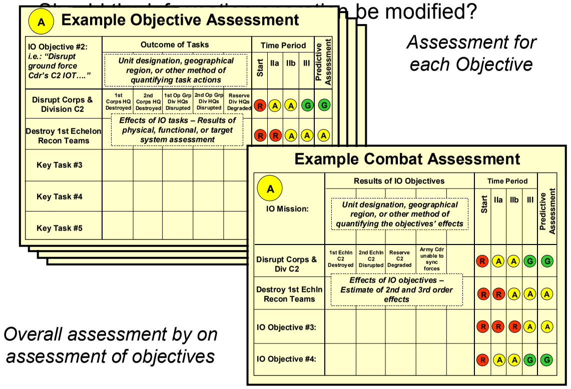
Format – MOE statements include:

- A *metric* - a standard of measurement such as a change in the info environment or adversary effort / technique, response or non-response.
- *What* data is to be observed, collected, & measured (in terms of number, time, etc).
- Example: Increase (*the metric*) of local populace support for friendly forces *(what is to be measured)*.

Combat Assessment (CA)

CA assesses the overall effect of the information operation (particularly in the cognitive domain) in order to determine whether IO is achieving its mission. Results are used to decide if the IO plan (concept of support) should proceed or change.

- CA is an aggregate of MOE assessments.
- CA answers the questions - What did IO do? Did IO achieve the desired effect in the cognitive domain? Should the information operation be modified?



A Example Objective Assessment

IO Objective #2: *i.e.: "Disrupt ground force Cdr's C2 IOT…."*	Outcome of Tasks *Unit designation, geographical region, or other method of quantifying task actions*					Time Period				Predictive Assessment
						Start	IIa	IIb	III	
Disrupt Corps & Division C2	1st Corps HQ Destroyed	2nd Corps HQ Destroyed	1st Op Grp Div HQs Disrupted	2nd Op Grp Div HQs Disrupted	Reserve Div HQs Degraded	R	A	A	G	G
Destroy 1st Echelon Recon Teams	*Effects of IO tasks – Results of physical, functional, or target system assessment*					R	R	A	A	A
Key Task #3										
Key Task #4										
Key Task #5										

Example Combat Assessment

A IO Mission:	Results of IO Objectives *Unit designation, geographical region, or other method of quantifying the objectives' effects*					Time Period				Predictive Assessment
						Start	IIa	IIb	III	
Disrupt Corps & Div C2	1st Echln C2 Destroyed	2nd Echln C2 Disrupted	Reserve C2 Degraded	Army Cdr unable to sync forces		R	A	A	G	G
Destroy 1st Echln Recon Teams	*Effects of IO objectives – Estimate of 2nd and 3rd order effects*					R	R	A	A	A
IO Objective #3:						R	R	R	A	A
IO Objective #4:						R	A	A	G	G

Assessment for each Objective

Overall assessment by on assessment of objectives

Appendix E

Training Considerations for Information Operations (IO)

General

Prior to establishing an IO training program, unit personnel should consult **FM 7-0, *Training the Force;*** **FM 7-1, *Battle Focused Training;*** **FM 3-0, *Operations;*** **FM 3-13, *Information Operations Doctrine, Tactics, Techniques, and Procedures;*** and **Joint Pub 3-13, *Joint Doctrine for Information Operations*** for tips on effective IO training.

Effective employment of IO depends on the ability to organize and train in the manner we will fight. What this means at the tactical level is that we train personnel directly responsible for executing the IO mission by integrating unit training throughout the live, virtual, and constructive environments; focusing on the area of operations (AO); and using a crawl-walk-run methodology culminating in a collective event stressing the IO team. While IO education can be taught separately, collective unit training should build on ongoing IO activities within the AO and transition to possible courses of action (COAs) responding to real-world contingencies, e.g., crisis deterrence, conflict resolution, etc. The intent of this appendix is to provide ideas and information for IO training. In the end, training IO is no different than training for other collective events, in that the basic tenants of Army training must be applied, which includes conducting an after-action review (AAR) after all training.

Unit training focusing on either offensive or defensive IO must consider all available and potential available capabilities, which include multinational, Department of Defense (DOD), and joint assets.

Normally, offensive and defensive IO training are integrated, emphasizing protection and defense of information and information systems. Therefore, when planning IO training, consider the appropriate scope and duration of the exercise. Remember, some IO capabilities fall outside the normal Army chain, and scripting of multinational, DOD, and joint capabilities need consideration. Thus, in order to obtain the true complexity of IO, you must incorporate those challenges of coordinating IO activities with other agencies, including nongovernmental.

Whenever possible, the commander accomplishes IO training through combined-arms operations. Even at the tactical level, the commander uses IO to disrupt or destroy enemy information systems through electronic warfare (EW) and physical destruction, which is most common at the brigade and battalion level. IO, applied correctly, is a combat multiplier that enhances the potential for friendly forces to defeat enemy forces in detail. The commander maintains access to his information system through operations security (OPSEC)/information security (INFOSEC) and electronic protection (EP). He seeks access to the adversary's system through counter-command and control (C2) and manipulates both systems to create a knowledge-based battlefield advantage that can be exploited by military forces to achieve the mission objective. Commanders who successfully plan and conduct IO significantly increase the potential of their force's combat power and control the tempo of the battle. IO is the means by which Army forces will fight and win the information war.

As you build your IO plan, consider the three methods for executing IO training: stand alone training, supported training, and supporting training. In stand alone training, your focus is on the adversary and your desire to affect the way he operates; that is, mitigating and interdicting his method of operating. You can use supported training when the focus is on IO in the main effort. There will be time when this is the case, so you ought to plan for this occasionally. Lastly, you can use supporting IO training when IO is applied as a force multiplier coupled with a conventional tactical operation, which is most of the time.

Essentials for Planning IO Training

The following considerations are fundamental for planning IO exercises. While this list is not all inclusive, it provides a basic road map for planning, conducting, and evaluating a unit exercise. For additional information on Army training, see **FM 7-0, *Training the Force,*** and **FM 7-1, *Battle Focused Training.***

- Determine the environment in which the training will take place: live, constructive, or virtual (see Chapter 4 of FM 7-1).
- Will the training leverage on-going unit training, and, if so, how will training integration take place?
- Develop concrete attainable IO objectives (see Chapter 3 of FM 7-1).
- Create a realistic IO environment attempting to emulate the unit's operating environment.
- Exercise all six IO activities in the context of the exercise.
- Provide for sufficient IO actions to support exercise objectives.
- Assess and evaluate IO employment.
- Exercise both offensive and defensive IO using all the capabilities available to the unit where it will operate.
- Exercise intelligence support to IO.
- Plan for and use appropriate security measures to protect IO tactics, techniques, and procedures (TTP).

Organization for Training

Whenever possible, the IO cell should have representatives from the targeting cell, targeting board, joint operations and targeting coordination board, or whatever integrating process the commander uses to integrate and synchronize his resources. If these assets are not available, scripting should be considered. Additionally, each element of command and control warfare (C2W), along with the civil affairs (CA) and public affairs (PA), should be represented as well. Replicating tactical combat operations, the targeting representative may become the focus of activity. When training, consider the functions of the IO, which are:

- Planning the overall IO effort for the commander.
- Developing IO concepts to support the scheme of maneuver.
- Establishing IO priorities to accomplish planned objectives.
- Determining the availability of IO resources to carry out plans.

Consolidated tasking will assist in the integration and synchronization required for effective IO. As the spectrum of engagement moves between peace to war and back again, it is appropriate to stand up an IO cell and exercise it. Listed below is a graphically diagramed notional IO cell for your consideration. The actual configuration depends on your situation and operational environment.

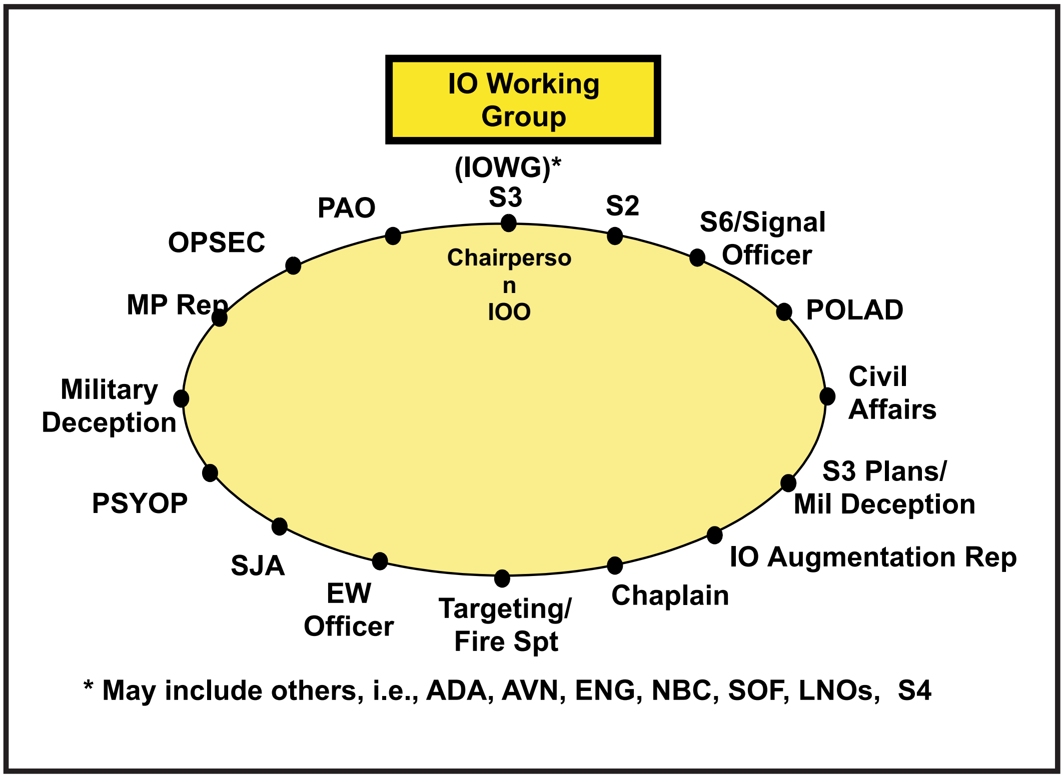


Figure E-1

Considerations for Training

Effective IO first requires specific information products on the adversary's military (C2, intelligence, and capabilities), social, religious, and economic background that may have to be provided by exercise planners. The data needed to create, update, and use these products needs to be built into the exercise scenario and master scenario events list.

Secondly, the opposition force should have an IO capability consistent with the exercise scenario. Realistic IO are essential to evaluating friendly IO.

Finally, consistent with the tenets of the exercise, free play of IO must take place by both Blue and Red forces. Pre-structured, mechanical IO will degrade the participant's ability to gain valuable experience from the demands of mental agility and creativity that unstructured IO can provide. Senior exercise participants should allow, even welcome, the C2 chaos that effective IO can cause to the exercise participants, and work through such problems.

Well before the exercise, you must develop a basic IO mission essential task list (METL) that includes tasks and subtasks. If it is possible, obtain the IO METL from the unit you may backfill in theater and compare the lists. Nevertheless, whatever list you develop, there must be tasks for each IO capability available to your unit. The IO METL enhances the objective of achieving information dominance at selected places and times during an operation. Consider the following tasks for inclusion:

- **Determining required IO information and how to get answers.**
  - Identify the commander's IO critical information requirements, priority intelligence requirements (PIR), and high-priority targets and synchronize intelligence and information plans and military plans on a near-real-time basis.
  - Establish information-linked strategic, operational, and tactical collection, fusion, and report processes (incorporating reconnaissance, surveillance, and target acquisition [RISTA]/sensor and counterintelligence [CI]/human intelligence [HUMINT] data) to develop continuous, timely IO intelligence preparation on the battlefield (IPB).
- **Knowing your IO capabilities and vulnerabilities in relation to the enemy, the natural environment, the political setting, international law, and so forth.**
  - Identify and prioritize IO essential elements of friendly information (EEFI).
- **Knowing enemy IO capabilities and vulnerabilities.**
  - Maintain a continuous IO estimate of potential adversaries and/or other operational situations in support of IO situational awareness and battlefield visualization.
  - Assess adversary command, control, communications, computers, and intelligence (C4I)/C2W operations, strengths, and vulnerabilities continuously.

- **Knowing how the enemy sees your capabilities and vulnerabilities in terms of IO, the battlefield, and PIR.**
  - º Understand the enemy's decision-making process.
  - º Identify the enemy's critical IO nodes.
  - º Develop enemy leader personality profiles.
  - º Understand the enemy's decision-making doctrine, tactics, and standing operating procedures (SOPs).
- **Protecting critical and vulnerable friendly IO.**
  - º Establish open-source processes to obtain, process, provide, secure, and release critical IO information, including PA, CA, governmental, and nongovernmental information, within legal and policy constraints.
  - º Establish and maintain critical, secure, intertheater/intratheater military communications and computer networks that support IO: for example, digitization, radar communication processor (RCP), situational awareness, battlefield visualization, distribution, and C2 across the battlespace.
  - º Assess friendly C2 vulnerabilities and C2; protect operations continuously and adjust to maintain C2 effectiveness.
  - º Achieve C2 protection in support of data integrity and infrastructure protection, IO/C2 node protection, spectrum superiority/control, and graceful degradation.
  - º Establish procedures to regain information dominance when it is discovered that the enemy has achieved information dominance.
- **Attacking critical enemy IO vulnerabilities.**
  - º Establish C2-attack targeting and battle damage assessment (BDA) and establish links to expedite dissemination of adversary information, to include timely sensor-to-shooter links.
  - º Attack, deny, degrade, exploit, and/or influence adversary C4I/C2W capabilities or other operations using lethal and nonlethal means.

(Note: Portions of the above information were extracted from Appendix D of **FM 3-13,** ***Information Operations Doctrine, Tactics, Techniques, and Procedures;*** and Chapter VI of **JP 3-13,** ***Joint Doctrine for Information Operations.)***

Appendix F

IO Targeting & Effects Aid

Key References

FM 6-20-10, *TTP for The Targeting Process* (MAY 96)

FM 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (NOV 03)

Key Definitions

Targeting: The process of selecting targets and matching the appropriate response to them, taking account of operational requirements and capabilities. (JP 1-02/FM 101-5-1)

Target: An area, complex, installation, force, equipment, capability, function, or behavior identified for possible action to support the commander's objectives, guidance and intent. (JP 3-60/FM 101-5-1)

Fires: The effects of lethal or non-lethal weapons. (JP 1-02)

Targeting Effects: The expected results of weapons against specific targets.

Field Support Division May 2004

Terms

High Value Target (HVT): A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. (JP 1-02)

High Payoff Target (HPT): A target whose loss will significantly contribute to the success of friendly courses of action. High-payoff targets are those high-value targets identified through war-gaming, which must be acquired and successfully attacked for the success of the commander's mission. (JP 1-02)

Essential Fire Support Task (EFST): A task for fire support to accomplish that is required to support a combined arms operation.

Essential Field Artillery Task (EFAT): A task for Field Artillery that must be accomplished to achieve an EFST.

Essential Information Operations Task (EIOT): A task for IO that must be accomplished to achieve an EFST.

Planning Fires and Effects for IO

MDMP	Targeting Action	IO Action
Mission Analysis	• Determine specified, implied, & essential fire support tasks • Determine HVTL • Translate fire support assets into capabilities • Develop draft targeting objectives or EFSTs	• Nominate targets to HVTL • Determine supporting IO capabilities • Develop IO objectives or EIOTs
COA Dev.	• Develop Concept of Fires (or Effects) • Develop initial HPTL • Quantify effects for EFSTs	• Input to Concept of Fires (or Effects) • Nominate targets to HPTL
COA Analysis & Comp.	• Finalize Concept of Fires • Finalize HPTL • Develop TSM • Develop fire support control measures	• Input to TSM
COA Approval	• Brief fire support plan as part of each COA	• None
Orders Prod.	• Write fires paragraph of & fire spt annex	• Cross-walk IO & fire spt annexes

Doctrinal Targeting Effects (FM 6-20-10)

The following are the standard "lethal" targeting effects used by the fire support element:

Limit – Reducing the options or courses of action available to the enemy commander.

Disrupt – Preclude effective interaction or the cohesion of enemy combat and combat support systems.

Delay – Alter the time of arrival of forces at a point on the battlefield or the ability of the enemy to project combat power from a point on the battlefield.

Divert – Tie up critical enemy resources.

Destroy – To render target a target so damaged that it cannot function as intended nor be restored to a useable condition without being entirely rebuilt.

Doctrinal Effects For IO (FM 3-13)

Destroy – Damage a combat system so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.

Disrupt – In information operations, means breaking or interrupting the flow of information between selected C2 nodes.

Degrade – In information operations, is using non-lethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems, and information collection efforts or means.

Deny – In information operations, entails withholding information about Army force capabilities and intentions that adversaries need for effective and timely decisionmaking.

Deceive – Cause a person to believe what is not true.

Exploit – In information operations, is to gain access to adversary command and control systems to collect information or to plant false or misleading information.

Influence – Cause adversaries or others to behave in a manner favorable to Army forces.

IO Input to the Targeting Cycle

Targeting Step	Actions
1 DECIDE	• Analyze the CDR's mission, intent, concept and initial planning guidance. • Develop input to targeting objectives. • Develop IO essential effects tasks which support the targeting objectives. • Determine which targets to engage (lethal and non-lethal) – how, when, & desired effect. • Provide input to Attack Guidance Matrix (AGM) or Targeting Synchronization Matrix (TSM). • Provide input to assessment plan.
2 DETECT	• Update the HPTL & AGM/TSM.
3 DELIVER	• Execute the engagement IAW the AGM/TSM.
4 ASSESS	• Evaluate if the desired effects were achieved. • Based on assessment, propose target re-engagement / changes to engagement scheme.

❶ DECIDE

PURPOSE: Provide an overall focus for targeting effects and set priorities for intelligence collection and engagement planning.

IO TASKS:

- In conjunction with the intelligence cells both inside targeting cell and the IO section (if available), identify known / emerging friendly and threat capabilities and vulnerabilities.
- Identify intelligence gaps in information environment analysis and refine IRs for inclusion in the collection manager's collection plan.
- Determine which threat vulnerabilities that must be attacked and friendly capabilities that must be protected in the information environment in order to achieve the desired effects.
- Identify and prioritize targets & target sets for IO. These targets are HVTs (i.e., key leaders, C2, civilian populace, threat groups, etc.).
- Determine the time (including duration) and place in the battlespace when the effect must be achieved to support the commander's scheme of maneuver.
- Provide this input to targeting objectives.

❷ DETECT

PURPOSE: Validate targets selected for engagement and identify other targets from information gained through the collection plan.

IO TASKS:

- Monitor execution of IO-related tasks in the ISR synchronization matrix / collection plan.
- Ensure targets of interest to IO are tracked.
- Modify the timing and priority of engagements and desired effects based on evolving situation.

❸ DELIVER

PURPOSE: Execution of the targeting plan in accordance with the TSM / ESM.

IO TASKS:

- In conjunction with the FECC/DOCC:
  - Ensure rationale for engagements is still valid.
  - Coordinate engagements as required.
- Collect BDA from executed engagements to feed into assessment efforts.
- Begin collection of MOP and MOE to feed into assessment efforts.

DECIDE (continued)

- Develop discrete Essential IO Tasks (EIOTs). EIOTs are key tasks that must be executed to achieve the commander's targeting objectives at the identified time and place. Available assets should be prioritized to execute these EIOTs above all other tasks.
- Identify target(s) which should be engaged to support identified EIOTs. These are HPTs
- Determine the desired effect for the EIOT. This should clearly identify what is to be accomplished by engaging the target.
- EIOTs should be written:

  Effect: Destroy, Degrade, Disrupt, Deceive, Deny, Influence, etc.

  Target / Target Set: The object of the intended effect.

  Purpose: The explanation of why the target set or target must be engaged.
- Develop a plan to assess IO effects and tasks.

This product produced by U.S. Army, 1st Information Operations Command (Land), Field Support Division

❹ ASSESS

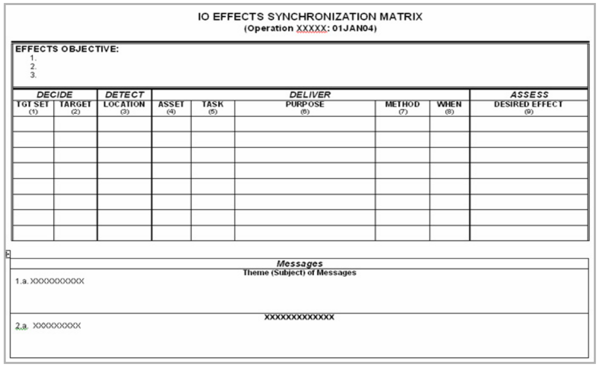
PURPOSE: Determine the overall effectiveness of the IO portion of the targeting plan. This effort should focus on objectives to determine if the desired effects are being achieved.

IO TASKS:

- Execute assessment plan:
  - Monitor the information environment in order to identify and assess indicators of change.
  - Monitor adversary actions and status for any indications that IO engagements are having an impact.
  - Monitor friendly forces' status for indications that adversary operations in the information environment are having success.
  - Determine the effectiveness of messages and how they should be refined for greater effect.
- Re-engagement Recommendation: Based on the assessment, determine if the target requires re-engagement and/or if the method of delivery, delivery asset or message requires modification.
- Adjustments to the engagement plan (TSM / ESM) as appropriate to accomplish the desired effects.

Target / Effects Synchronization Matrix (TSM / ESM)

- Tool for planning and synchronizing lethal and non-lethal engagements.
- The TSM / ESM is produced by FECC/DOCC, with input from the IO section and the battle staff.



IO EFFECTS SYNCHRONIZATION MATRIX
(Operation XXXXX: 01JAN04)

EFFECTS OBJECTIVE:
1.
2.
3.

DECIDE		DETECT	DELIVER					ASSESS
TGT SET (1)	TARGET (2)	LOCATION (3)	ASSET (4)	TASK (5)	PURPOSE (6)	METHOD (7)	WHEN (8)	DESIRED EFFECT (9)

Messages
Theme (Subject) of Messages

1.a. XXXXXXXXXX

XXXXXXXXXXXXX

2.a. XXXXXXXXX

NOTE: Representative example; formats vary by command, but the same type information will be presented. IO targets and engagements should be embedded in the planning products to improve synchronization.

Writing MOE

- Each IOET should have one or more MOE.
- Use the task's purpose as a guide to what must be observed, reported, and assessed.
- MOE should include both objective and subjective metrics to make a more holistic evaluation of success.
- Subjective MOE should be observable, quantifiable, precise, and correlated to the effect of the IOET.
- Objective MOE should be directly tied to the IOET, and gives the commander a direct input into assessment.
- If an MOE is difficult to write for a particular IOET, then re-visit the IOET to ensure it has a clearly defined, attainable effect. Re-write if necessary.

Format – MOE statements include:

- A *metric* - a standard of measurement such as a change in the info environment or adversary effort / technique, response or non-response.
- W*hat* data is to be observed, collected, & measured (in terms of number, time, etc).
- Example: Increase (*the metric*) of local populace support for friendly forces *(what is to be measured).*

Example MOE:

- (Subj) Level of paramilitary influence on the populace.
- Percentage of positive / neutral /negative articles published in local newspapers.

CALL PUBLICATIONS INFORMATION PAGE

In an effort to make access to our information easier and faster, we have put all of our publications, along with numerous other useful products, on our World Wide Web site. The CALL Web site is restricted to Department of Defense personnel. The URL is http://call2.army.mil.

If you have any comments, suggestions, or requests for information, you may contact CALL by using the Web site "Request for Information" or "Comment" link. We also encourage Soldiers and leaders to send in any tactics, techniques, and procedures (TTP) that have been effective for you or your unit. You may send them to us in draft form or fully formatted and ready to print. Our publications receive wide distribution throughout the Army, and CALL would like to include your ideas. Your name will appear in the byline.

Contact us by:

PHONE: **DSN 552-3035/2255; Commercial (913) 684-3035/2255**
FAX: **Commercial (913) 684-9564**
MESSAGE: **CDRUSACAC FT LEAVENWORTH, KS // ATZL-CTL//**
MAIL: **Center for Army Lessons Learned**
ATTN: ATZL-CTL
10 Meade Ave, Building 50
Fort Leavenworth, KS 66027-1350

Additionally, we have developed a repository, the CALL Archives, that contain a collection of operational records (OPORDS and FRAGOS) from recent and past military operations. Much of the information in the CALL Archives is password-protected. You may obtain your own password by accessing our Web site and visiting the CALL Archives page. Click on "Restricted Access" and "CALL Archives Access Request." After you have filled in the information and submitted the request form, we will mail you a password. You may also request a password via STU III telephone or a SIPRNET e-mail account.

CALL's products are produced at Fort Leavenworth, KS, and are not distributed through publication channels. Due to limited resources, CALL selectively provides its products for distribution to units, organizations, agencies, and individuals and relies on them to disseminate initial distribution of each publication to their subordinates. Contact your appropriate higher element if your unit or office is not receiving initial distribution of CALL publications.

Installation distribution centers
Corps, divisions, and brigades
Special Forces groups and battalions
Ranger battalions
Staff adjutant generals

TRADOC schools
ROTC headquarters
Combat training centers
Regional support commands

CALL PRODUCTS "ON-LINE"

Access information from CALL via the World Wide Web (www). CALL also offers Web-based access to the CALL Archives. The CALL Home Page address is

http://call.army.mil

CALL produces the following publications:

BCTP Bulletins, CTC Bulletins, Newsletters, and Trends Products: These products are periodic publications that provide current lessons learned/TTP and information from the training centers.

Special Editions: Special Editions are newsletters related to a specific operation or exercise. Special Editions are normally available prior to a deployment and targeted for only those units deploying to a particular theater or preparing to deploy to the theater.

News From the Front: This product contains information and lessons on exercises, real-world events, and subjects that inform and educate Soldiers and leaders. It provides an opportunity for units and Soldiers to learn from each other by sharing information and lessons. ***News From the Front*** can be accessed from the CALL Web site.

Training Techniques: Accessed from the CALL products page, this on-line publication focuses on articles that primarily provide tactics, techniques, and procedures (TTP) at the brigade and below level of warfare.

Handbooks: Handbooks are "how to" manuals on specific subjects such as rehearsals, inactivation, and convoy operations.

Initial Impressions Reports: Initial impression reports are developed during and immediately after a real-world operation and disseminated in the shortest time possible for the follow-on units to use in educating personnel and supporting training prior to deployment to a theater. Products that focus on training activities may also be provided to support the follow-on unit.

To make requests for information or publications or to send in your own observations, TTP, and articles, please use the CALL Request For Information (RFI) system at http://call-rfi.leavenworth.army.mil/. There is also a link to the CALL RFI on each of our major Web pages, or you may send email directly to:

callrfi@leavenworth.army.mil

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