

**UNITED STATES MARINE CORPS**  
MARINE CORPS CIVIL-MILITARY OPERATIONS SCHOOL  
WEAPONS TRAINING BATTALION  
TRAINING COMMAND  
2300 LOUIS ROAD (C478)  
QUANTICO, VA 22134-5036

## **STUDENT OUTLINE**

### **INFORMATION OPERATIONS**

**0530-108**

**CIVIL AFFAIRS OFFICER COURSE**

**M020A3D**

**FEBRUARY 2016**

## **LEARNING OBJECTIVES**

a. **TERMINAL LEARNING OBJECTIVE**. Given a mission, Commander's intent, and access to Interorganizational and local representatives, coordinate with interorganizational agencies, local authorities and related capabilities, to build international support, conserve resources, and conduct coherent operations in accordance with MCWP 3-33.1 Ch. 4. and to ensure the CMO effort is synchronized and coordinated with other related staff functions such as information operations, public affairs, and military information support operations in accordance with MCWP 3-33.1 Chapter 2. (CACT-EXE-2009)

### b. **ENABLING LEARNING OBJECTIVES**

(1) Without the aid of references, identify MISO capabilities that are organic to the MAGTF, in accordance with MCWP 3-40.4. (CACT-EXE-2009o)

(2) Without the aid of references, identify the information related capabilities, in accordance with the MCWP 340.4. (CACT-EXE-2009p)

(3) Given a scenario, integrate information operations into Civil-Military Operations planning, in accordance with JP 3-57 Ch III. (CACT-EXE-2009q)

1. **INFORMATION ENVIRONMENT (IE)**. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive.

a. **Defining the Information Environment**

(1) The Physical Dimension. The physical dimension is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to: human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablets, etc. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries.

(2) The Informational Dimension. The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information.

(3) The Cognitive Dimension. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals or groups processing information, their perception, judgment, and decision making capabilities. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies. Defining these influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects. As such, this dimension constitutes the most important component of the information environment.

(4) The information environment is not an exclusively military one. In fact, the military applications of information are almost obscured in today's universal usage of the

information spectrum by national, international, and non-state players.

(5) In an information environment, military conflicts consist of interactions between humans and technology. Success is measured by indications that the effects created are influencing the enemy, friendly, and/or neutral activities in the desired ways on the battlefield.

b. **Visualizing the Information Environment (IE)**

(1) The Operating Environment: The operating environment can refer to a number of things: High ground, saddles, fields of fire, aiming points and METT-TSL (Mission, Enemy, Terrain and Weather, Troops and Fire Support Available, Time Available, Space, Logistics) type information. This describes a portion of the physical dimensions, but not in terms of the IE. It is a good starting point and is something with which most are familiar.

(2) The Physical Dimension of the IE. The Physical Dimension is defined as the material part of the information environment. It overlaps with the land, sea, air, and space domains where military maneuver and combat operations occur and where the physical elements of information systems and the networks that connect these systems reside and operate.

(a) Key characteristics of the physical dimension include those important to maneuver operations: geography (terrain), weather, populace, and civil infrastructure (to include communication networks and media).

(b) These characteristics affect the employment of information system assets and the linking of information systems into networks.

(c) Key individuals: leaders, their advisors, family members.

(d) Some examples include:

1. Human networks: Tribal, religious, families, business, governmental, educational, security, informants.

2. Technical: Computers, printing presses, radios, antennas, cameras, control panels, C2 systems, internet.

3. Physical: Media centers, universities and schools, bunkers, Gov/Medical/phone facilities, Religious/Financial institutions.

(3) The Information Dimension of the IE. You can begin to understand how complicated the IE is. The Information Dimension is an abstract concept based on theory. It possesses a dual nature that consists of information itself. However it also serves as the medium by which information is collected, processed, and disseminated (i.e. the functions of information systems).

(a) Key characteristics include those essential to information management and command and control (C2): Information quality (completeness, accuracy, timeliness, relevance, and consistency), distribution (range, sharing, and continuity), and interaction (exchange or flow of information).

(b) These characteristics affect information content and the functions of information systems.

(c) Content: Truths, propaganda, rumors, disinformation, misinformation, themes, storylines, talking points, images that support goals of a group or individual, organization's critical information.

(4) The Cognitive Dimension of the IE. The definition of the Cognitive dimension is: A level of abstract construct that exists in the human mind and incorporates the collective consciousness of groups and organizations. This domain includes intangibles such as morale, unit cohesion, and level of training, experience, public opinion, and situational awareness. The cognitive dimension is where decisions are made.

(a) Some of the key characteristics of the cognitive dimension are those that affect both individual and collective (organizational) decision-making: Perceptions (attitudes), awareness (opinions, beliefs, and values), and understanding (knowledge).

(b) What does the individual or individuals believe? How did the individual or individuals develop that belief? What decisions will an individual or individuals decide to make?

2. **INFORMATION OPERATIONS (IO) DEFINITIONS**

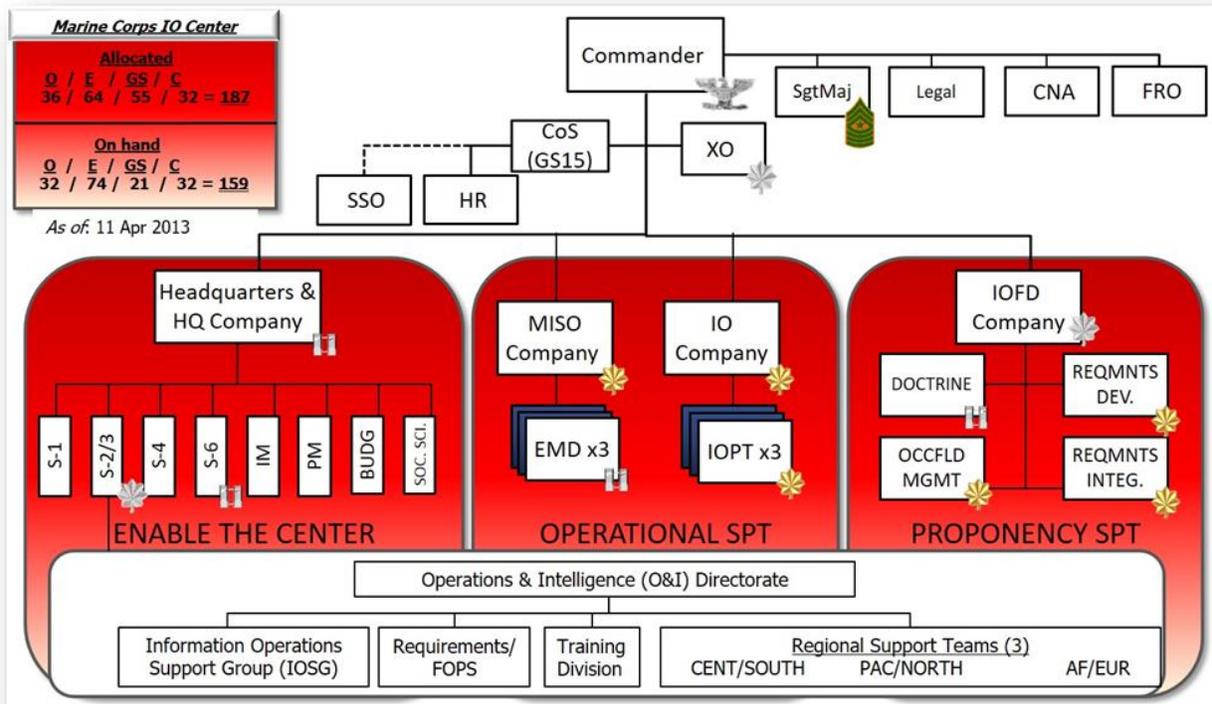
a. **Joint Information Operations (IO) Definition.**

Information operations is the integrated employment, during military operations, of Information-Related Capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. (JP 3-13/JP1-02)

b. **Marine Corps Definition of Information Operations.**

Information operations is defined as the integration, coordination, and synchronization of all actions taken in the information environment to affect a relevant decision makers behavior in order to create an operational advantage for the Commander. (MCWP 3-40.4)

3. **MARINE CORPS INFORMATION OPERATIONS CENTER (MCIOC).** Mission Statement: The MCIOC provides operational support to the Marine Forces (MARFOR) and Marine Air-Ground Task Forces (MAGTF) and provides Information Operations (IO) subject matter expertise in support of USMC IO advocates and proponents in order to enable the effective integration of IO into Marine Corps operations.



a. **MCIOC Support Construct - MISO Capabilities Organic to the MAGTF.** MCIOC has multiple deployable teams to support

Information Operations in the MAGTF. The Expeditionary MISO Teams support tactical level Military Information Support Operations. The IO Planning Teams support the MAGTF HQ by providing links to interorganizational IO Capabilities. They also provide skilled IO planners to better integrate the Information Related Capabilities to support the Commander's objectives.

b. **MAGTF IO Capability:** IO Company (~ 30 Marines)

- (1) IO Planning Team (MEU) (2 Pax)
- (2) IO Planning Team (MEB) (4 Pax)
- (3) IO Planning Team (MEF) (4-6 Pax)

c. **MAGTF MISO Capability:** MISO Company (~ 80 Marines)

- (1) Expeditionary MISO Team (EMT) (3 Pax)
- (2) Expeditionary MISO Detachments (EMD) (13 Pax)

MEU	MEB	MEF
1 x IOPT (2 PAX) 1 x EMT (3 PAX)	1 x IOPT (4 PAX) 1 x EMD (13 PAX) for each RCT	1 x IOPT (4-6 PAX) 1 x EMD (13 PAX) for each RCT
<u>R2P2</u> : Recognition, general assumptions, pre-packaged effects, playbook/check-list	<u>MCPP</u> : Deliberate planning, deeper thought, longer timeline, IRs, specific, tailored/task organized, MOE/MOPs	
<ul style="list-style-type: none"> <li>✓ Link to IO training (individual/collective, steady-state/PTP)</li> <li>✓ Link to Joint, Interagency, Intergovernmental, Multi-national (JIIM) IO capability <ul style="list-style-type: none"> <li>○ J-39s, Navy &amp; MARFOR IO <ul style="list-style-type: none"> <li>• Read into Regional Programs, Voice Program Actions &amp; Assessments, ACCMs</li> </ul> </li> <li>○ Regional Information Support Teams (RIST)</li> <li>○ NIOC/IWC <ul style="list-style-type: none"> <li>• Human dimension focus</li> </ul> </li> </ul> </li> <li>✓ IO and Information-related Capability (IRC) focused planning <ul style="list-style-type: none"> <li>○ Advanced knowledge of the Information Environment</li> <li>○ Working to detailed level knowledge of IRCs (to include SAPs)</li> <li>○ Reach back/through to develop unique products and leverage external resources</li> </ul> </li> <li>✓ Tactical dissemination of approved MISO products</li> <li>✓ Interface with OPFOR to coordinate operational needs/requirements (MCCLL, UNS, etc.)</li> </ul>		

4. **INFORMATION-RELATED CAPABILITIES (IRCs)**. IRCs are the tools, techniques, or activities that affect any of the three dimensions of the information environment. They affect the ability of the Target Audience (TA) to collect, process, or disseminate information before and after decisions are made. The TA is the individual or group selected for influence. The joint force (means) employs IRCs (ways) to affect the information provided to or disseminated from the TA in the physical and informational dimensions of the information environment to affect decision making. The change in the TA conditions, capabilities, situational awareness, and in some cases, the inability to make and share timely and informed decisions, contributes to the desired end state. Actions or inactions in the physical dimension can be assessed for future operations.

a. **Key IRCs**. IO is not about ownership of individual capabilities, but rather the use of those capabilities as force multipliers to create a desired effect. There are many military capabilities that contribute to IO and should be taken into consideration during the planning process.

(1) **Operations Security (OPSEC)**. OPSEC is a standardized process designed to meet operational needs by mitigating risks associated with specific vulnerabilities in order to deny adversaries critical information and observable indicators. OPSEC identifies critical information and actions attendant to friendly military operations to deny observables to adversary intelligence systems. Once vulnerabilities are identified, other IRCs (e.g. military deception, cyberspace operations) can be used to satisfy OPSEC requirements. OPSEC practices must balance the responsibility to account to the American public with the need to protect critical information. The need to practice OPSEC should not be used as an excuse to deny noncritical information to the public.

(2) **Military Deception (MILDEC)**. One of the oldest IRCs used to influence an adversary's perceptions is MILDEC. MILDEC can be characterized as actions executed to deliberately mislead adversary decision makers, creating conditions that will contribute to the accomplishment of the friendly mission. While MILDEC requires a thorough knowledge of an adversary or potential adversary's decision-making processes, it is important to remember that it is focused on desired behavior. It is not enough to simply mislead the adversary or potential adversary; MILDEC is designed to cause them to behave in a manner advantageous to the friendly mission, such as misallocation of

resources, attacking at a time and place advantageous to friendly forces, or avoid taking action at all.

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

(4) Cyberspace Operations (CO). Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace capabilities, when in support of IO, deny or manipulate adversary or potential adversary decision making, through targeting an information medium (such as a wireless access point in the physical dimension), the message itself (an encrypted message in the information dimension), or a cyber-persona (an online identity that facilitates communication, decision making, and the influencing of audiences in the cognitive dimension). When employed in support of IO, CO generally focuses on the integration of offensive and defensive capabilities exercised in and through cyberspace, in concert with other IRCs, and coordination across multiple lines of operation and lines of effort.

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

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

(6) Information Assurance (IA). IA is necessary to gain and maintain information superiority. The JFC relies on IA to protect infrastructure to ensure its availability, to position information for influence, and for delivery of information to the adversary. Furthermore, IA and CO are interrelated and rely on each other to support IO.

(7) Physical Security. Physical security is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. Physical security contributes directly to information protection. Information, information-based processes, and information systems—such as C2 systems, weapon systems, and information infrastructures are protected relative to the value of the information they contain and the risks associated with the compromise or loss of information.

(8) Counter Intelligence. Counterintelligence is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. Counterintelligence is the intelligence function concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion, or terrorism. The principal objective of counterintelligence is to assist with protecting friendly forces. Counterintelligence enhances command security by denying adversaries information that might be used against friendly forces and to provide protection by identifying and neutralizing espionage, sabotage, subversion, or terrorism organization or efforts.

(9) Special Technical Operations (STO). IO needs to be deconflicted and synchronized with STO. Detailed information related to STO and its contribution to IO can be obtained from the STO planners, usually at Service Component Headquarters. IO

and STO are separate, but have potential crossover, and for this reason an STO planner is a valuable member of the IO cell.

(10) Civil-Military Operations (CMO). The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational U.S. objectives.

(11) Combat Camera (COMCAM). Combat camera is the acquisition and utilization of still and motion imagery in support of operational and planning requirements across the range of military operations and during exercises. Official visual documentation is used for operational and combat support as well as public information purposes. It is an essential visual record of Marine Corps commands throughout significant and often historical events. Complete access to areas of operations and timely exploitation of collected imagery are key to COMCAM success.

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

(13) Military Information Support Operations (MISO). MISO are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. MISO focuses on the cognitive dimension of the information environment where its TA includes not just potential and actual adversaries, but also friendly and neutral populations. MISO are applicable to a wide range of military operations such as stability operations, security cooperation, maritime interdiction, noncombatant evacuation, foreign humanitarian operations, counterdrug, force protection, and counter-trafficking. Given the wide range of activities in which MISO are employed, the military information support representative within the IO cell should consistently interact with Public Affairs (PA), CMO, Joint Interagency Coordination Group (JIACG), and IO planners.

(a) MISO capabilities at the Operational Level. At the operational level, MISO can include the distribution of leaflets, radio and television broadcasts, and other means of transmitting information that provide information intended to influence a selected group. It may be used to encourage adversary forces to defect, desert, flee, surrender, or take any other action beneficial to friendly forces.

(b) MISO capabilities at the Tactical Level. At the tactical level, MISO enables the tactical commander to directly communicate and empathize with target audiences. Tactical level MISO includes face-to-face contact and the use of loudspeakers or other means to deliver MISO messages. MAGTF MISO is predominately focused on the tactical level.

(c) Expeditionary MISO Team (EMT). An EMT generally consists of a MISO team chief (staff sergeant or sergeant), an assistant team chief (sergeant or corporal), and an additional Marine to serve as a gunner and to operate the speaker system. A team is equipped with a vehicle fitted with a loud speaker, and often works with a local interpreter. The CA Team is most likely to encounter or work with an EMT when deployed.

(14) Public Affairs (PA). PA comprises public information, command information, and public engagement activities directed toward both the internal and external publics with interest in the DoD. External publics include allies, neutrals, adversaries, and potential adversaries. When addressing external publics, opportunities for overlap exist between PA and IO.

b. CMO, PA and IO. All IRCs must to work together to get the most out of each and every activity. The IO officer convenes an IO Working Group (IOWG) to provide integrated IO input to Operational Planning Team (OPT) efforts. CMO and PA should have a seat at the table. The tactical level is where much of the relevant IO battle is fought and won.

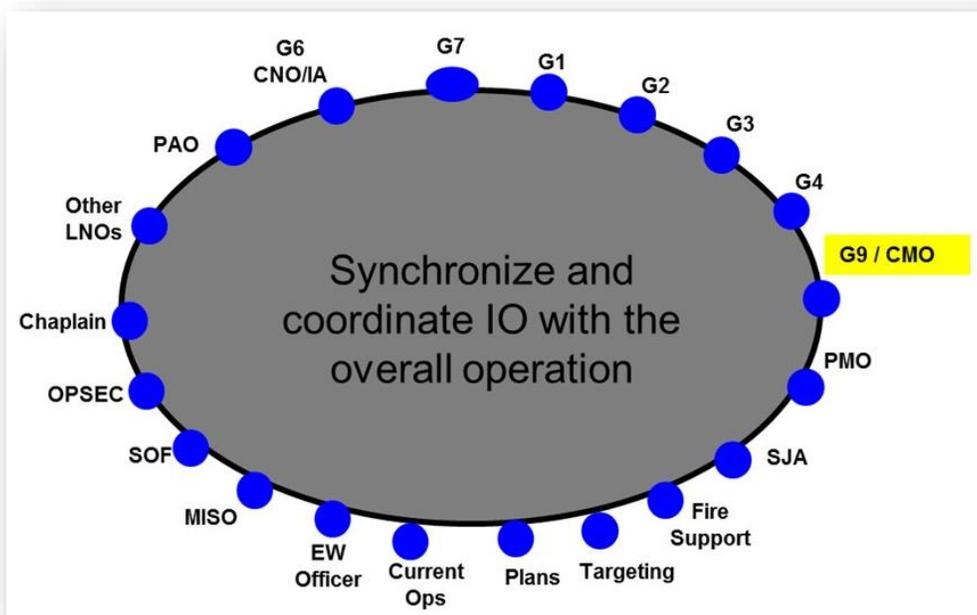
## 5. CMO INTEGRATION WITH IO

a. CMO can directly affect and be affected by IO. CMO activities establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to achieve U.S. objectives. These activities may occur prior to, during, or subsequent to other military operations.

In CMO, personnel perform functions normally provided by the local, regional, or national government, placing them into direct contact with civilian populations. This level of interaction results in CMO having a significant effect on the perceptions of the local populace. Since this populace may include potential adversaries, their perceptions are of great interest to the IO community. For this reason, CMO representation in the IO cell can assist in identifying TAs, synchronizing communications media, assets, and messages, and providing news and information to the local population.

b. Although CMO and IO have much in common, they are distinct disciplines. The TA for much of IO is the adversary; however, the effects of IRCs often reach supporting friendly and neutral populations as well. In a similar vein, CMO seeks to affect friendly and neutral populations, although adversary and potential adversary audiences may also be affected. This being the case, effective integration of CMO with other IRCs is important, and a CMO representative on the IO staff is critical. The regular presence of a CMO representative in the IO cell will greatly promote this level of coordination.

c. **Information Operations Working Group (IOWG)**. IOWG coordinates the information operations activities amongst the staff, and synchronizes activities and actions with higher headquarters. By including the IOWG into the battle rhythm, it by necessity will be deconflicted with other staff meetings and will facilitate attendance by Liaison Officers (LNOs) and other members of the staff to include the CMO staff element (G-9).



6. **CMO AND IO.** IO can support CMO in almost any Civil-Military Operation by influencing, developing, or controlling the indigenous population. CMO complements IO in numerous ways by providing feedback on the effectiveness of IO activities and products. CMO also provides valuable input to IO and MISO planners based on direct interaction with the population. Two examples of CMO support to IO are support to military operations and support to civil authorities.

a. **Support to Military Operations.** CMO supports military operations by minimizing civilian interference with military operations, maximizing support for operations, and meeting the commander's legal and moral obligations to civilian populations.

(1) Operationally, CMO supports national policy and implements U.S. national objectives by coordinating with, influencing, developing, or accessing indigenous populations.

(2) Tactically, CMO works to secure local acceptance of and support for U.S. forces. It is important to IO; because, CMO involves interfacing with essential organizations and individuals in the AO and with Non-Governmental Organizations (NGOs) and Intergovernmental Organizations (IGOs).

b. **Support to Civil Authorities (SCA).** CMO support to civil authorities includes assistance with relief and dislocated civilian support and security. These activities may include such actions as:

(1) Coordinating the removal of civilians from the combat zone.

(2) Interfacing between U.S./multinational forces and host nation and other IGOs/NGOs.

(3) Exercising military control over an area, hostile government, or population.

7. **HOW CA METHODOLOGY CONTRIBUTES TO IO.** CA Methodology contributes to IO in the following manner:

a. **MCPD Problem Framing**

(1) CPB analysis provides valuable data and insight that aid in development of the Combined Information Overlay (CIO).

(2) The application of ASCOPE/PMESII during the decide phase (CA Methodology) helps focus CA assets on essential aspects of the IO campaign.

(3) During a civil assessment, you don't just collect information on infrastructure you are also assessing the people, their moods, attitudes, and how they feel about the Host Nation Government and U.S. Forces; all valuable information to CA Planners. You may also be able to find out what is the best method for MISO to get their message out.

b. **Example of Combined Information Overlay.** As the example demonstrates there are many areas that the information you develop in the CPB process and the IO/MISO planners develop overlap and complement one another.

UNCLASSIFIED

## EXAMPLE CIO

<p><b>Physical:</b>          Population: 100K; Main population Amungme Tribe/People          Weather: 84-86 degrees; moderate rain; currently dry season          Terrain: Mountain Ridge from N to S on the West, Tropical terrain to South, Arafura Sea to the East          Transportation: Moses Kalangin Airport (all aircraft capable), Helo pad scattered throughout the city and nearby port; 2 ports- Amanpare, Timika (capable of handling container ships and ferries          Roads: Hard surfaced, centered around Timika, connects ports and mine and power plant          Utility: Coal power plant          Industry: Agriculture- coffee, coconut, corn and casawa; Tourism          Communication: Radio Network, Satellite TV, Local Newspaper, Satellite Internet Connectivity</p>	<p>Timika Afd. Timika Papua, Indonesia          Timika a.          Timika Papua, Indonesia          © 2012 TerraMetrics          © 2012 Tele Atlas          Image © 2012 DigitalGlobe          Imagery Date: 2/27/2007 2007          11°55'00"S 136°53'17.60"E elev. 55 m</p>
<p><b>Informational:</b> Timika has (1) radio station Gemma FM (106.3) broadcasts from Timika. Unknown if national Indonesian FM RRI stations can reach Timika. Timika Pos is the only local print media, it does not publish in English (likely Bahasa Indonesian but unknown). Regional print media distribution is unknown. FCX base has satellite phone and internet access, but external media access in the rest of the village is unlikely. Regional cellular statistics indicate that 95% of the Province is covered with 2G coverage (Teleksom) and it is likely that Timika has 3G coverage as it is a larger village with a large population of regional migrants. Free to air TV covers RRI public messaging, external media comes from internet and satellite communications. FCX dominant narrative: situation is calm and investors have nothing to worry about. TNI/BRIMOB external narrative: keep status quo, we are here just for security of TCNs. Internal narrative: here to secure mining profits for Gol. Ethnic Papua short term: stop human rights violations, follow through on sharing mining profits with Papua. OPM Long term: Papua as its own country through violence.</p>	
<p><b>Cognitive:</b> Capital of Mimika regency and contains the majority of the residents. Ethnically mixed; Papuan (Amungme), Indonesian (Java Sumatran), and TCNs (as well as AMCITS). Timika is less isolated and more prone to outside influence given its proximity to the airfield and port. Those living here have been heavily influenced by the West, including dress and behavior. A majority Muslim population in a historically Christian dominated area, it is a fair assumption that some conflict can be based on ethnic differences with both political and economical impacts. Power is structured around mine employment (PT Freeport), traditional clan family structures, and local government appointments. Largest employer is PT Freeport, though the vast majority of Indonesian Nationals employed by the company have been resettled from other parts of Indonesia via the Government's trans-migration program. Key Influencers: NGOs, Religious Organizations, Alfo Rafal (Mayor), LtCol T. Suandnyana (Timika Air Force Base Commander), 754<sup>th</sup> Infantry Bn / 3d Assault Cav Leadership, PT Freeman Indonesia Management, Tembapapura Tribal/Clan Leader, BRIMOB.</p>	

**IO Considerations:** The diverse nature of the dense population, geography, and weather norms will hinder the means, methods, and perceptions of disseminating messages to the populace; friendly or enemy. In the way of indigenous information distribution, radio, social networks (internet), local newspapers, and regular gatherings (face to face meetings) at mosques, churches, and market centers, all serve as reliable conduits to the populace. Newspapers are printed daily by 12 different companies for the 78% of the literate population, but the bias and credibility to the populace is still unknown. Cell phone coverage is over 95% of the country with both 2G and 3G services making them a likely means of information passing and gathering. Protests and violence have impacted travel in and around Timika, likely affecting local services (to include communications). Western influence is perceived to have a significant impact, which may aid in the credibility of any messages. However, care must be taken to ensure that we are not perceived as siding with PT Freeport, or showing bias towards big businesses at the expense of locals. Strikes and protests facilitated by an opportunistic OPM are an effort to bring attention to the plight of the Papuan people, as well as an attempt to seize power and attention from Gol.

UNCLASSIFIED

▲ = YYY/POLRI  
 ■ = XXX Activity/Unrest  
 ★ = AMCIT/TCN

c. **Example of an IO Tasking Worksheet.** Note: CMO is one of the areas the IO Planner is supposed to develop tasking for. It is best if this is done in a collaborative manner. This way you can ensure (as much as possible) that tasks supporting CMO are included, as well as task supporting IO are de-conflicted with CMO objectives and tasks.

<b>Command Objective:</b> Shape environment to accept our presence and our narrative		<b>MOE</b>
<b>IO Objective (Target + Impact):</b> XXX establishes neutral or supportive position towards U.S. presence and objectives		
<b>IO Task = Action + Target + Purpose</b>		
MISO	Influence XXX affiliates to accept the U.S. as credible, committed and unbiased in in promoting peaceful resolution to regional issues IOT prevent hostile acts	Decrease in disruptive OPM activities
EW	BPT disrupt XXX C2 IOT prevent coordinated response to MEB actions	
MILDEC		
OPSEC	Deny XXX/YYY information on friendly forces IOT prevent disruption of MEB operations	
CNO	Exploit XXX networks IOT monitor XXX attitudes towards MEB efforts	<b>MOEI</b>
Phys ATK	BPT disrupt XXX C2 IOT prevent coordinated response to MEB actions	Fewer protests, roadblocks, violence
Phys SEC		
CI	Identify subversive XXX members IOT reduce opposition to MEB efforts	
IA	Protect friendly networks IOT prevent usurpation of MEB narrative	
COMCAM	Documents operations IOT support portrayal of MEB legitimacy and impartiality	<b>HPTs</b>
PAO	Informs XXX of MEB goals of stability, neutrality, and objectivity toward political factions within the AO IOT avoid perception of partiality	OPM Ldrshp
CMO	Coordinate NGO/IGO/OGA efforts IOT establish the opportunity for the XXX to communicate with the coalition	
DSPD	Informs XXX of MEB objectives and intentions IOT establish communications and reinforce impartiality	

## 8. **LIMITATIONS**

a. As with any capability, if it is poorly understood it will lead to incorrect perceptions of what Information Operations can and cannot achieve.

b. The need of CA forces to maintain credibility with the civil populace limits the extent to which they can support IO. If not they risk losing the support or cooperation of NGO/PVO and the populace.

c. CA soldiers collect information and conduct assessments in order to target their relief efforts or stabilize the civil environment.

d. The daily encounters between CA Marines and the people and institutions of the area of operations (AO) are prime

sources of information. However if they staff does not have effective communication the MAGTF staff sections can't benefit from it.

e. Internal integration should take place via the IO Working Group and the CMO Working Group.

f. CA Marines should not actively or knowingly participate in activities (MILDEC, Intel, etc.) that can damage their credibility or reputation with the populace.

9. **COORDINATION TASKS RELATING TO IO.** The G-9 (CMO) provides coordination tasks that relate to IO. They include:

a. Recommend CMO-related information requirements and Essential Elements of Friendly Information (EEFI) to the IO Officers.

b. Coordinate with the Intelligence Officer on aspects of the enemy situation that may affect CMO.

c. Coordinate for tactical forces to perform CMO tasks through the Operations Officer.

d. Coordinates with the IO Officer on trends in public opinion.

e. Coordinate with the IO Officer and Public Affairs Officer (PAO) to ensure disseminated information is truthful and supports IO objectives and themes.

f. Coordinates with the PAO on supervising public information media

g. Coordinate with the PAO and MISO to leverage media assets in the AO (press releases/interviews).

**REFERENCE:**

JP 3-13 Information Operations

JP 3-13.2 Military Information Support Operations, 2011

MCWP 3-40.4 MAGTF Information Operations, 2013

MCO 3120.20 Marine Corps Information Operations Program, 2008

