ATP 3-13.1

THE CONDUCT OF INFORMATION OPERATIONS

OCTOBER 2018

Headquarters, Department of the Army

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil/) and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

Army Techniques Publication
No. 3-13.1

Headquarters
Department of the Army
Washington, DC, 04 October 2018

The Conduct of Information Operations

Contents

Figures

Tables

This page intentionally left blank.

Preface

ATP 3-13.1, *The Conduct of Information Operations*, provides guidance on conducting information operations (IO) at tactical through strategic echelons and across operational phases. It is primarily intended for IO officers and planners or those assigned responsibilities for fulfilling IO duties. Secondarily, it is a useful primer for commanders, operations officers, intelligence officers, and other staff members who oversee, coordinate, or support IO planning, preparation, execution, and assessment.

The principal audience for ATP 3-13.1 is all members of the Army Profession. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States, international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement (see FM 27-10).

ATP 3-13.1 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms. This publication seeks to minimize using acronyms but will use two acronyms routinely: IO for information operations and IRC for information-related capability. If other acronyms are employed, their use will be limited to the paragraph or section in which they appear, or a legend will be available.

ATP 3-13.1 applies to the Active Army, Army National Guard)/Army National Guard of the United States, the United States Army Reserve, and the Army Civilian Corps unless otherwise stated.

The proponent for this publication is the U.S. Combined Arms Center, Information Operations Proponent Office. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send written comments and recommendations on a DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, United States Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCD (ATP 3-13.1), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; by e-mail to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Acknowledgements

This publication's discussion of social media in Chapter 3 is derived from Ian Tunnicliffe and Steve Tatham's "Social Media—The Vital Ground: Can We Hold It?" in *The Letort Papers*: U.S. Army War College Press, 2017. This publication is in the public domain.

Some of the terminology and thinking included in Chapters 4 and 6 (the logic of the effort and the theory of change) is courtesy of the RAND Corporation's *"Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners"* by Christopher Paul, Jessica Yeats, Colin P. Clarke, Miriam Matthews, and Lauren Skrabala. 2015.

This page intentionally left blank.

Introduction

ATP 3-13.1, *The Conduct of Information Operations*, provides Army leaders and information operations (IO) professionals with essential information necessary to integrate IO effectively into their unit's operation. It guides leaders to synchronize information-related capabilities (IRCs)—such as military information support operations, cyberspace electromagnetic activities, military deception, and operations security—to achieve effects in and through the information environment that support the commander's intent and concept of operations. The techniques discussed are deemed a way to conduct IO, not the way. Army professionals tailor the processes, tools, and techniques of IO to suit the mission, situation, and requirements of their commanders.

Commanders, subordinate leaders, and all members of the Army Profession ensure they conduct IO in accordance with the moral principles of the Army Ethic. They perform and accomplish IO ethically, effectively, and efficiently, mindful of applicable laws, policies, regulations, and procedures (see ADRP 1 for more on the Army Profession).

ATP 3-13.1 contains seven chapters and one appendix. The following is a brief description of each:

Chapter 1 provides an overview of the conduct of information operations. It discusses methods by which staffs at company through corps and above affect the information environment to a decisive advantage but with differing levels of expertise, supporting capabilities, and authorities. The chapter reviews a range of characteristics that distinguish the conduct of IO at higher versus lower levels.

Chapter 2 provides a technique for analyzing, understanding, and visualizing the information environment. Because IO largely concerns creating effects in this environment, it is essential to understand it in all its complexity.

Chapter 3 discusses determining the IRCs available to a unit and methods to request other capabilities, if required. The chapter also provides a brief synopsis of the various IRCs that commanders and staffs synchronize to create effects in the information environment.

Chapters 4 examines techniques for integrating and synchronizing information-related capabilities. It begins by discussing commanders' responsibilities and transitions to discussing staffs' responsibilities. It also provides samples of a range of tools and products commonly employed by commanders and staffs to ensure the right effects are generated at the right place and time.

Chapter 5 discusses intelligence support to IO, which is essential to its conduct. It also provides an overview of the ways that IO is integrated into the targeting process.

Chapter 6 overviews assessment, starting with its framework and then discussing its focus, types, and components. It provides techniques for developing IO objectives, measures of performance, measures of effectiveness, and indicators, as well as for presenting assessment results to the commander.

Chapter 7 examines the conduct of IO across operational phases and how these phases align with joint phasing.

Appendix A provides an overview of IO in garrison and available joint and Army IO-related training.

This page intentionally left blank.

Chapter 1
Information Operations Terms and Considerations

INFORMATION OPERATIONS TERMINOLOGY

1-1. Understanding information operations (IO) begins with understanding the terminology used to discuss it. *Information operations* is the integrated employment, during military operations, of information-related capabilities 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). An *information-related capability* is a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions (JP 3-13). Examples of information-related capabilities (IRCs) include military information support operations (MISO), military deception, operations security, public affairs, electronic warfare (EW), civil affairs operations (CAO), and cyberspace operations (see chapter 3 for an expanded discussion of IRCs).

1-2. Army commanders conduct IO to affect the information environment. The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). Staffs support commanders by synchronizing the employment of IRCs to gain an advantage over an enemy, an adversary, or a threat in the information environment. This advantage contributes to achieving the commander's intent, executing the concept of operations by countering and ultimately defeating the enemy or adversary's ability to operate in the information environment, and protecting and preserving friendly freedom of action in an operational environment to gain and maintain positions of advantage.

1-3. Information is an element of combat power. Units conduct IO to maximize the impact of the information element on operations. Leaders of IO units consider the following:

- IO focuses on affecting decision making. First it influences, usurps, corrupts, or destroys the enemy or adversary's ability to make timely, accurate, and relevant decisions. Second it protects, preserves, and enhances the leader's ability to make timely, accurate, and relevant decisions.
- Commanders are responsible for the conduct of IO. They are supported by their staffs and, depending on the mission or situation, by all members of the unit.
- IO synchronizes IRCs to create effects in the information environment that, in turn, shape and affect an operational environment.

1-4. The conduct of IO requires commanders, staffs, and particularly the IO officer or designated representative to—

- Analyze, understand, visualize, and describe an operational environment with specialized focus on the information environment, including—
  - The threat's use of the information environment.
  - Relevant stakeholders (those who affect friendly and threat decision making or are affected by it).
- Determine available IRCs and understand what each brings to the fight; request additional capabilities, as required.
- Plan IO as part of the operations process.
- Develop supporting products and input to plans and orders, such as combined information overlays, synchronization matrixes, an IO running estimate, and Appendix 15 (IO) to Annex C (for an example of an IO appendix, see FM 3-13).
- Establish and conduct an IO working group or otherwise coordinate with staffs, IRCs, and unified action partners to create effects in the information environment.

- Synchronize IRCs.
- Coordinate intelligence support to IO.
- Integrate IO into the targeting process.
- Assess IO within the operations assessment process.

These elements are continuous, cyclical, and iterative (see chapters 3 and 4 for additional details).

INFORMATION OPERATIONS CONSIDERATIONS ACROSS ECHELONS

1-5. IO supports operations from company level to Army Service component command (ASCC) level and above; however, the conduct of IO differs at each level. IRCs that an ASCC can employ are more expansive than a battalion can employ. Still, both echelons have the same responsibility to create effects in and through the information environment in their operational areas.

1-6. Factors that differentiate the conduct of IO from the lowest through the highest levels include—

- The supported operations and objectives.
- The size and complexity of the information environment.
- The presence of organic IO expertise.
- Tasks, knowledge, and skillsets required of IO personnel.
- Availability of IRCs.
- Access to staff support forces and reachback.
- Authorities and legal considerations.

SUPPORTED OPERATIONS AND OBJECTIVES

1-7. The type of operation and its objectives that IO supports vary with echelon. An *operation* is a sequence of tactical actions with a common purpose or unifying theme (JP 1) to achieve one or a limited set of objectives whose attainment is necessary to achieve the mission. *Unified land operations* are simultaneous offensive, defensive, and stability or defense support of civil authorities tasks to seize, retain, and exploit the initiative to shape the operational environment, prevent conflict, consolidate gains, and win our Nation's wars as part of unified action (ADRP 3-0). Unified land operations shape the information environment for IO. At higher echelons, the operations occurring are larger, more numerous, and more complex, as is the number of objectives being pursued. Also at higher levels, IO may be a major component of the lines of operation, its own line of effort, and in support of other lines of effort for a given operation.

SIZE AND COMPLEXITY OF THE INFORMATION ENVIRONMENT

1-8. The size and complexity of the information environment varies with echelon. The information environment—comprising individuals, organizations, and systems that collect, process, disseminate, or act on information—has three dimensions: physical, informational, and cognitive. The information environment is global but can be described in the context of regions and operational areas. It is both bound by culture, language, access to technology, and customs and traditions, and unbound in that information can readily flow into and out of a region or operational area into the global environment. The environment of an ASCC is considerably larger and more complex in physical and informational terms than an environment of a battalion. Yet, in terms of the cognitive dimension of this environment, similar challenges—such as how best to influence relevant audiences and to affect enemy or adversary decision making—exist at all echelons.

PRESENCE OF ORGANIC INFORMATION OPERATIONS EXPERTISE

1-9. Echelons vary in how much organic IO expertise they contain. IO officers and elements are currently found at the division level through ASCC. Whether or not an IO officer is assigned to a unit does not eliminate the responsibility of commanders at all levels to conduct IO. Commanders at brigade and below must, therefore, assign IO responsibilities to someone in their unit and ensure this individual receives the requisite training necessary to plan, prepare, execute, and assess IO (see appendix A for information on IO training).

TASKS, KNOWLEDGE, AND SKILLSETS REQUIRED OF INFORMATION OPERATIONS PERSONNEL

1-10. The tasks, knowledge, and skillsets required of IO personnel vary by echelon. IO is challenging at all levels; however, the knowledge and skillsets necessary to conduct IO at brigade and below differs from the knowledge and skillsets necessary to conduct IO at echelons above brigade. At brigade and below, IO personnel are responsible for synchronizing a smaller, less technical array of IRCs than are IO officers at division and above. IO personnel at division and above also prepare to operate in a more complex information environment and against advanced threat information systems. Some IO personnel at division and above work as part of a joint force and alongside unified action partners with whom they must achieve common objectives in the information environment.

AVAILABILITY OF INFORMATION-RELATED CAPABILITIES

1-11. The availability of IRCs in IO varies depending on the echelon supported. All units can conduct activities or employ capabilities that—

- Support the commander's task to inform and influence audiences inside and outside an organization.
- Affect enemy or adversary decision making, such as military deception.

Units at all echelons support the commander's task by maintaining a presence, profile, and posture; ensuring operations security; and conducting Soldier and leader engagement. However, the availability of IRCs—in the form of specific expertise, units, operations, and activities—is more limited at brigade and below. For example, space and cyberspace operations capabilities are not readily available to battalions unless requested well in advance and approved by higher headquarters.

ACCESS TO STAFF SUPPORT FORCES AND REACHBACK

1-12. Access to staff support forces and reachback required from IO personnel vary by echelon. When an IO staff lacks the required personnel, knowledge, or skillsets to conduct the tasks assigned to it, the command requests support. This support can come from individual augmentation to fill an approved manning document, by attaching small elements to the IO staff, or by designating a supporting unit that provides a needed capability through reachback. When filling individual augmentation billets or attaching elements to the staff, the command fills from its higher headquarters before requesting support from external units. For example, a corps or division staff that is not deployed may fill out a brigade or battalion staff that is deployed. When external support is necessary, the following units typically provide it:

- 1st Information Operations Command (Land), Active U.S. Army.
- 56th Theater Information Operations Group (TIOG), Washington State Army National Guard.
- 71st TIOG, Texas Army National Guard.
- 151st TIOG, United States Army Reserve.

1st Information Operations Command (Land)

1-13. The 1st IO Command, a major subordinate command of the U.S. Army Intelligence and Security Command, is a brigade-sized, multicomponent unit. Under the operational control and tasking authority of the U.S. Army Cyber Command, it provides distinctly tailored IO and cyberspace operations planning, synchronization, assessment, and reachback support to the Army and other military forces. Consisting of a headquarters and headquarters detachment and two battalions, it augments military forces with tailored IO and cyberspace operations support provided through deployable teams, cyber-opposing forces support, reachback planning and analysis, Army mission readiness exercises, and specialized training to assist units in garrison, during exercises, and during contingency operations.

1-14. The 1st IO Command also supports the Army by working to optimize IO interoperability with joint forces, other military forces, various agencies, and allies. It provides expeditionary cyberspace operations support to help units identify network vulnerabilities and enable IO.

Theater Information Operations Groups

1-15. The Army relies upon TIOGs to provide enhanced IO planning, synchronization, and assessment support to Army echelons from theater and ASCC to brigade levels. Three TIOGs exist:

- The 56th TIOG, U.S. Army National Guard, Fort Lewis, Washington.
- The 71st TIOG, U.S. Army National Guard, Camp Mabry, Texas.
- The 151st TIOG, U.S. Army Reserve, Fort Totten, New York.

Each TIOG consists of a group headquarters, a headquarters and headquarters company, and two IO battalions that have the capability to provide IO field support teams or general field support teams.

1-16. The TIOGs and their battalion elements do not deploy as commands but instead form and deploy purpose-built IO field support teams designed to provide the necessary IO support required by the requesting command. To enhance the capabilities of the field support teams and reduce preparation time, the TIOGs maintain regional focuses. These focuses help provide the supported command with additional regional expertise and capabilities to plan, synchronize, and assess IRCs when conducting IO in the area of operations. Having a regional focus, however, does not preclude a TIOG from deploying IO teams and providing IO support to organizations and commands outside of its regional focus area (see FM 3-13 for more detail on these organizations).

AUTHORITIES AND LEGAL AND ETHICAL CONSIDERATIONS

1-17. Some capabilities integrated and synchronized by the IO officer or designated representative—such as MISO, cyberspace electromagnetic activities, and integrated joint special technical operations (known as IJSTO)—are governed by authorities that dictate parameters or constraints on their employment. While these IRCs tend to reside at higher levels, brigades and below may be impacted by their respective constraints, particularly when these capabilities are augmenting or supporting their operations. Commanders—with advice from IO officers, public affairs officers, IRC representatives, and judge advocate general (known as JAG) officers—make themselves aware of these limitations that affect lead times and dictate how effects will be achieved. When such capabilities are authorized, the best way to understand the parameters or constraints under which units must operate is to request a capabilities briefing from the IRC unit commander or senior representative (see DODD 3600.01 as a starting point for these considerations).

1-18. As trusted Army professionals and stewards of the Army Profession, all commanders, staffs, and IO professionals strive to make right decisions and take actions that enable them to conduct IO ethically, effectively, and efficiently.

Chapter 2
Information Environment Analysis

INTELLIGENCE PREPARATION OF THE BATTLEFIELD AND INFORMATION OPERATIONS

2-1. The information environment is the aggregate of three components—individuals, organizations, and systems—that collect, process, disseminate, or act on information. Understanding this environment requires an analyst—chiefly the IO officer or designated representative—to analyze each component of the environment as well as their aggregate. The analyst determines how the components interrelate.

2-2. The information environment also has three dimensions: physical, informational, and cognitive. All are important. The physical dimension consists of what users see—the physical content of the environment. This dimension contains observable behavior. This behavior enables the commander and staff to measure the effectiveness of their efforts to influence enemy and adversary decision making and the attendant actions that must occur across all audiences in the area of operations (AO). The informational dimension is the code that captures and organizes information that occurs in the physical dimension so that it can be stored, transmitted, processed, and protected. This dimension links the physical and cognitive dimensions. The cognitive dimension consists of the perspective of those who inhabit the environment; their individual and collective efforts to give context to what is happening or has happened and make sense of it. In this dimension, sense making occurs. If conflict is ultimately a contest of wills and victory is achieved by defeating the enemy or adversary psychologically, then achieving effects in the cognitive dimension can be decisive. The cognitive dimension is the hardest to understand. Therefore, the better that units operate in and exploit the physical and informational dimensions, the more they can overcome the challenges associated with the cognitive dimension. Table 2-1 on page 2-2 explores the three dimensions.

2-3. One purpose of IO involves affecting an adversary's ability to make sense of unfolding events. Affecting the adversary's perception of an event can indirectly impair, disrupt, or disable the adversary's ability to lead and direct operations. At the same time IO affects those perceptions, it attempts to preserve friendly commanders' ability to lead their forces and understand, visualize, describe, and direct operations. IO uses social media—a dominant aspect of the information environment—across and among all three dimensions. Messages, images, graphics, and sounds transmitted via social media affect perceptions and behaviors in real time and with profound impact.

2-4. Actions that occur in an operational environment almost always create effects in all three dimensions of the information environment. Through effective, proactive planning, units account for intended primary, secondary, and tertiary effects to support the commander's intent and concept of operations, while mitigating unintended effects. Precise effects across all three dimensions are only possible if the unit commander analyzes, understands, and visualizes the information environment and operational environment as a whole. Even the most prepared staff cannot anticipate all potential effects; however, understanding the information environment enables the staff to prepare for and react to unintended effects and determine why they occurred.

2-5. The mechanics of analyzing the information environment and enemy or adversary operations in the information environment are generally the same as those established to support intelligence preparation of the battlefield (IPB) for other military planning. IPB is a critical component of the military decisionmaking process (MDMP). It provides a systematic approach to evaluating the effects of significant characteristics of an operational environment for missions (for a full discussion of IO and the MDMP, see FM 3-13). IPB to support IO refines traditional IPB to focus on the information environment. Its purpose is to gain an understanding of the information environment in a geographic area and determine how the enemy or adversary will operate in this environment. The focus is on analyzing the enemy's or adversary's use of information to gain positions of relative advantage. The end state is the identification of threat information

capabilities in the information environment against which friendly forces must contend and threat vulnerabilities that friendly forces can exploit with IO.

Table 2-1. Information environment dimensions

Types	*Affects*	*Examples*
Physical	Content	• The physical world and its content, particularly that which enables and supports exchanging ideas, information, and messages. • Information systems and physical networks. • Communications systems and networks. • People and human networks. • Personal devices, handheld devices, and social media graphical user interface. • Mobile phones, personal digital assistants, and social media graphical user interfaces.
Informational	Code	• Collected, coded, processed, stored, disseminated, displayed, and protected information. • Information metadata, flow, and quality. • Social media application software, information exchange, and search engine optimization. • The code itself. • Any automated decision making.
Cognitive	Context	• The impact of information on the human will. • The contextualized information and human decision making. • Intangibles, such as morale, values, worldviews, situational awareness, perceptions, and public opinions. • Mental calculations in response to stimuli, such as liking something on a social media application.

2-6. In addition to the running estimate, IPB to support IO results in producing a graphic or visualization product known as the combined information overlay. This overlay results from a series of overlays that depict where and how information aspects such as infrastructure, content, and flow potentially affect military operations. In certain instances, staffs may need more than one combined information overlay to capture the full complexity of the information environment (see paragraph 2-50 for a discussion on combined information overlay).

2-7. During mission analysis, the IO officer or representative ensures that IPB addresses the information environment and supports the planning and execution of operations. The intent is to better visualize the impact of the information environment on unit operations and to identify potential threat capabilities and vulnerabilities that the unit can protect against or exploit. This analysis involves four substeps that mirror the steps discussed in ATP 2-01.3:

- Define the information environment.
- Describe the information environment's effects.
- Evaluate the threat's information situation.
- Determine threat courses of action in the information environment.

STEP 1: DEFINE THE INFORMATION ENVIRONMENT

2-8. During the first step of mission analysis, the IO officer or representative coordinates with other staff officers and elements, particularly the intelligence staff section. Defining the information environment begins by clearly delineating the AO, as well as areas of interest, including contiguous areas to the AO that may affect information flow and decision making. Once delineated, the IO officer identifies the significant characteristics of the information environment within this defined area in all three dimensions (physical, informational, and cognitive) that can affect friendly and threat operations, as well as influence friendly

courses of action and command decisions. These significant characteristics can include, but are not limited to, the following:

- Terrain (and weather).
- Populace.
- Societal structures.
- Military or government information and communications infrastructure.
- Civilian information and communications infrastructure.
- Media.
- Third party organizations.

TERRAIN (AND WEATHER)

2-9. One characteristic that the IO officer identifies is the terrain (and weather). The IO officer looks at the various ways physical, geographical, and atmospheric aspects of the AO impact information content and flow. These aspects can include compartmentalization, canalization, signal attenuation, radio wave propagation, and atmospheric and environmental limits on employing information systems.

POPULACE

2-10. Populace is another characteristic that the IO officer identifies. This characteristic involves identifying the human composition of the AO or area of interest in all its diversity to determine factors that impact information flow, receipt, and understanding. These factors tend to be static and non-voluntary; they are enduring traits or patterns of behavior that are innate or culturally ingrained to the point they are habitual and non-reflexive. Often IO officers study demographic and linguistic factors such as age, gender, education level, literacy, birth rate, ethnic composition, family structure, employment or unemployment rates, and languages.

SOCIETAL STRUCTURES

2-11. Societal structures affect friendly and threat operations. IO officers identify human networks, groups, and subgroups that affiliate along religious, political, or cultural lines, including commonly held beliefs and local narratives. These affiliations are voluntary and varied—over time, over space, and among individuals. IO officers focus their analysis on preferred means, methods, and venues that each social affiliation uses to interact and communicate and the ways each collectively constructs reality. Analysis examines biases, pressure points, general leanings, and proclivities, especially as they pertain to support or opposition of friendly and adversarial forces. Analysis also explores how these networks, groups, and subgroups express themselves and their commonly held beliefs through written and spoken narratives, stories, and messages.

MILITARY OR GOVERNMENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

2-12. The IO officer identifies another characteristic: the military or government information and communications infrastructure. Details of this characteristic involve understanding informational networks and communications systems that move information through the information environment to support military and governmental activities and facilitate decision making. Key networks and systems include special or enclave telecommunications means, methods, and capacity, such as telecommunications towers, fiber-optic networks, telephone networks (wired or wireless), microwave, satellite, and internet. IO officers understand the type and volume of information passed over or through these systems. These officers also benefit from knowing military or governmental authorities (leaders, decision makers, and military and civilian workforce) who use, manage, and control these systems.

CIVILIAN INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

2-13. A related characteristic that the IO officer identifies is civilian information and communications infrastructure. This characteristic involves understanding informational networks and communications systems servicing the general population that move information throughout the information environment. Key systems include telecommunications towers, fiber-optic networks, telephone networks (wired or

wireless), microwave, satellite, internet, and cellular networks. IO officers identify these systems and the informational content moved on them before understanding ways that forces—friendly or adversarial—can exploit these systems to influence indigenous populations.

MEDIA

2-14. Characteristics of media can affect friendly and threat operations. Media includes physical, informational, and cognitive means by which local populations (including the adversary) receive and have their thinking shaped by information. Examples of the media's characteristics include radio and television broadcast facilities; print production facilities; news reporting, production, and dissemination sources; and outlets servicing the AO and areas of interest. Other examples include the primary and backup information systems used to move information from point to point, the information reported in terms of volume and content, the media's range and distribution capabilities, the audiences being marketed to and affected by the media, and the observed bias of the media and its cognitive effect on government, military, and civilian leaders, decision makers, and the general population.

THIRD-PARTY ORGANIZATIONS

2-15. Third-party organizations also have characteristics that affect operations. These organizations that simultaneously message in the information environment vary from nongovernmental and private organizations to other government agencies and international organizations. IO officers place analytical emphasis on identifying these organizations, determining their audiences, discerning their agendas, and estimating their impact on friendly operations.

2-16. Identifying and defining the significant aspects of the information environment helps to focus the IPB to support IO on those characteristics that will influence friendly courses of action (COAs) and command decisions. This focus thereby prevents unnecessary analysis and wasted effort. The initial analysis in this step determines the resources and time the IO officer or element commits to the detailed analysis that occurs in Step 2.

STEP 2: DESCRIBE THE INFORMATION ENVIRONMENT EFFECTS

2-17. In this step, the IO officer examines the significant characteristics or features of the information environment identified in Step 1 and determines their potential effects or impacts on friendly and threat operations in each dimension. As with IPB in general, this step focuses on how the threat, terrain and weather, and civil considerations can affect operations.

DESCRIBE HOW THE THREAT CAN AFFECT FRIENDLY OPERATIONS

2-18. The enemy or adversary is part of an operational environment and information environment. The threat's physical posture alone influences friendly decisions and operations, as well as the decisions and actions of the populace in the AO in ways that benefit the threat commander's intent.

2-19. For many adversaries, the information environment is decisive terrain. Adversaries actively seek to shape it to their advantage, often well before hostilities begin. Although a detailed analysis of enemy forces occurs during Step 3 and Step 4 of the IPB process to support IO, Step 2 defines the type of enemy forces and their general information capabilities. This is done to place the existence of these forces and their capabilities in context with other variables to understand their relative importance to the information environment. Sometimes the mere presence of a threat force is the most important characteristic in the information (as well as operational) environment. This force presence is the chief locus of influence. In other instances, the presence or absence of communications infrastructure or other feature will be the predominating characteristic.

2-20. The results of this substep are typically reflected in threat and situational overlays, which are visual depictions of doctrinal and current physical dispositions of all potential threat information forces or capabilities in the AO and area of interest. In addition to locations, these graphics include the identity, size, strength, AO, and coverage or reach for each potential threat information unit or capability. The IO officer

often supplements these overlays with a threat description table that describes the threat's broad information capabilities (see Steps 3 and 4 of the IPB process for additional information about these overlays).

DESCRIBE HOW TERRAIN AND WEATHER CAN AFFECT FRIENDLY AND THREAT OPERATIONS

2-21. *Terrain analysis* is the collection, analysis, evaluation, and interpretation of geographic information on the natural and man-made features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations (JP 2-03). Just as terrain can canalize friendly or threat movement and maneuver, it can canalize the flow of information, thereby affecting the timeliness and effectiveness of decision making. Weather analysis is the evaluation of the direct and indirect effects of weather and climate on operations in the information environment. These effects can be as simple as directly affecting the employment of capabilities, such as EC-130J Commando Solo, or as complex as indirectly affecting AO-wide efforts to inoculate the local populace against enemy propaganda.

2-22. Terrain analysis involves identifying obstacles and key terrain, but IPB to support IO analyzes these features in terms of how they will affect the employment of IRCs, the flow of information, and decision making. Similarly, IPB to support IO analyzes weather patterns, forecasts, and climate data to determine their impact on IRC's employment, information flow, and decision making.

DESCRIBE HOW CIVIL CONSIDERATIONS CAN AFFECT FRIENDLY AND THREAT OPERATIONS

2-23. An understanding of civil considerations enhances the selection or formulation of IO objectives, the weighting of IO efforts (attack, defend, or stabilize), the appropriate mix of IRCs, and their employment, among other aspects. Such understanding begins even before deployment and leverages the entire staff, as well as outside agencies and unified action partners, who has relevant regional knowledge and expertise in civil considerations.

2-24. One method to discern significant civil consideration characteristics is depicted in table 2-2 on page 2-6, which crosswalks civil considerations with operational variables. Operational variables are known by the acronym PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, and time). Civil considerations, a subset of mission variables—mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (known as METT-TC)—comprise areas, structures, capabilities, organizations, people, and events (known as ASCOPE). Staffs use operational variables to develop a comprehensive understanding of operational and information environments. Civil considerations refine this understanding so that staffs can visualize and describe operational and information environments in a manner that fosters shared understanding. This crosswalk helps the IO staff refine its understanding of what is relevant to missions and operations from its perspective. The staff can complete it with any single mission variable to the operational variables (see appendix A of FM 6-0 for information about operational variables; see chapter 4 ATP 2-01.3 for information on specific civil considerations in the IPB process).

Table 2-2. Examples of operational variables crosswalked with civil considerations

	Political	*Military*	*Economic*	*Social*	*Information*	*Infrastructure*
Areas	• Enclave, province, district • National boundaries • Shadow government influence area	• Areas of influence and interest • Area of operations • Safe haven • Local nation base or training area	• Commercial • Fishery • Industrial • Markets • Mining • Smuggling routes • E-commerce	• Refugee camp • Ethnic, social, tribal enclave • School district • Online group	• Broadcast coverage area • Social media reach or penetration • Word of mouth • Graffiti	• Road system • City limit • Power grid • Irrigation network • Suburb, exurb, urban core
Structures	• Court house • Government center • Capitol building • Meeting hall	• Base and base buildings • Training facility • Known leader house	• Banking • Fuel • Factory • Warehousing • Online store • “Wall Street” versus “Main Street”	• Club • Jail • Library • Religious building • Restaurant • Social media platform	• Cell tower • Broadcast facility • Physical internet structure • Postal service • Print shop	• Emergency shelter • Public building • Airfield, bridge, railroad • Construction sites • Electric station
Capabilities	• Civil authority, practices and rights • Executive, legislative, and judicial functions • Dispute resolution	• Doctrine • Organization • Training • Materiel • Leadership • Personnel • Facilities • Civil-military relationship	• Currency • Food security • Market or black market • Raw material • Tariff • BITCOIN • Imports or exports	• Social network • Nonprofit support to disasters • Social services	• News operation • Newspaper • Social media platform • Literacy rate • Intelligence service • Internet access	• Law enforcement • Fire fighting • Maintenance • Transportation • HVAC (heating, ventilation, and air conditioning)
Organizations	• Major political party • Nongovern-mental organization • Host government • Court system • Insurgent group affiliation	• Host-nation forces • Insurgent group or network • Terrorist • Military lobbying group	• Bank • Business organization • Guild • Labor union • Landowner • Cooperative	• Clan • Online or in-person affinity group • Patriotic or service organization • Familial	• Media group • Public relations firm • Social media information group • News organization	• Construction company • Trade union • Cooperative

Table 2-2. Examples of operational variables crosswalked with civil considerations (*continued*)

	Political	*Military*	*Economic*	*Social*	*Information*	*Infrastructure*
People	• United Nations representative • Political leader • Governor • Elder • Legislator, judge, and prosecutor	• Key leader • Thought leader	• Banker • Employer or employee • Employment rate • Merchant • Smuggler	• Community leader • Teacher • Entertainer • Criminal • Migration patterns	• Decision maker • Elder • Religious leader • Internet personality	• Builders • Local development council • Road repairers • Police, fire fighter
Events	• Election • Council meeting • Treaty signing • National parade • Speech • Significant legal trial	• Combat • Military parade • Unit relief • Loss of leadership	• Drought, yield • Labor migration • Market day • Payday • Business opening	• Celebration • Civil disturbance • Funeral • Online forum • Social media livestream	• Censorship • Publishing dates • Online launch • Press briefing • Interview • Disruption of service	• Scheduled maintenance • School construction • New bridge opening • Disaster, man-made or natural

2-25. Due to the complexity and volume of data involving civil considerations, no simple or single model exists for presenting this analysis. It typically comprises a series of products, such as data files, overlays, and assessments.

2-26. IO officers and planners often use one common technique to present analysis. They prepare an overlay (graphical depiction) for each significant characteristic that visually displays its salient features and identifies gaps in intelligence or information that are subsequently refined into requirements for collection (requests for information, requests for collection). Figures 2-1 and 2-2 on pages 2-8, 2-9, and 2-10 provide example overlays. The first focuses on population centers and the second focuses on communications infrastructure. Both examples are based on the Decision Action Training Environment or DATE scenario as employed at the Joint Readiness Training Center.

Note. These overlays depict "a" way, not "the" way. IO officers or representatives must adapt their products to the situation at hand, their units' standard operating procedures, and commander's preference.

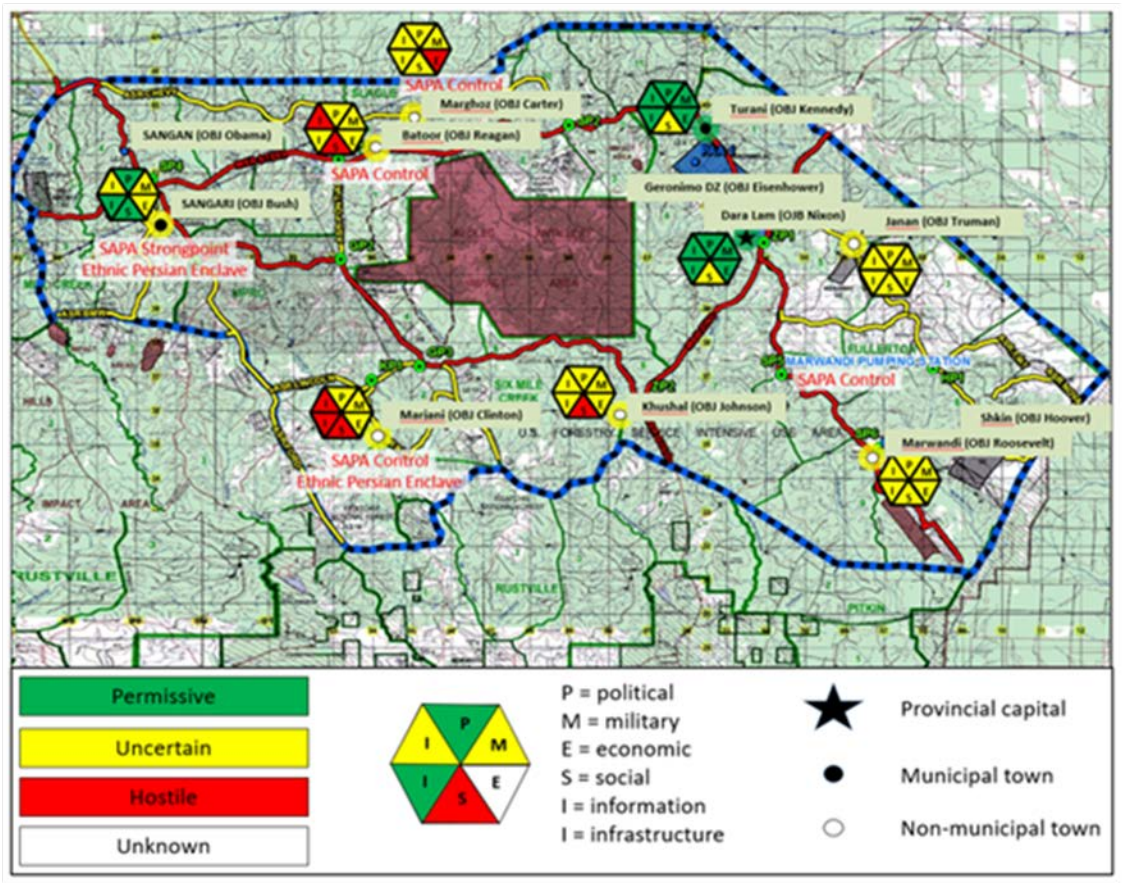

Figure 2-1. Example overlay that depicts relevant information about the populace in the area of operations

Sangari: • 2nd largest town in Kirsham • Strong allegiance to ROA (pre-SAPA) • Active municipal gov. (pre-SAPA) • ROA/U.S. built 'Model City" • Regular access to school, medical facility, and emergency services • Many businesses • Majority ethnic Persian; minimal ethnic tension pre-SAPA • SAPA restricts information flow	***Turani:*** • Joint municipality with Dara Lam • Strong allegiance to ROA • Strong economic growth • Majority ethnic Atropian • Moderate inter-ethnic friction • Adequate transportation • USAID and NGO activity • Clinic funded and operated by town (USAID rehabilitation project)	***Janan:*** • Small rural village • Dependent on NGO/IGO for essential services • Agricultural economy; minimal growth • Majority ethnic Atropian; dislike SAPA/likely support anti-SAPA activity • Ethnic unrest; Persian residents likely support insurgents/resent U.S. presence • Inadequate transportation
Batoor: • Small rural village • Active local gov. (pre-SAPA) • Majority ethnic Atropian strongly dislike SAPA/support anti-SAPA activity • Ethnic groups polarized; Persian residents likely resent U.S. mil. • Subsistence agriculture (pre-SAPA); some work for pipeline company • Atroprian-funded medical clinic; mobile NGO medical/food aid (pre-SAPA) • SAPA severely restricts information • Provincial water treatment facility	***Dara Lam:*** • Kirsham Provincial Capital and largest most prosperous town • U.S. Consulate • Strong allegiance to ROA • Strong economic growth • Majority ethnic Atropian • Moderate inter-ethnic friction • Adequate transportation • Access to schools, medical, emergency services • Sadvol enclave	***Khushal:*** • Small rural village • Active local government • Majority ethnic Atropian; strongly dislike SAPA/support anti-SAPA activity • Polarized population; Persian-Atropian tensions actively exploited by SAPA • ROA funded med clinic/school; mobile med/food aid (NGOs) • Subsistence agriculture/livestock; some work for pipeline company
Marghoz: • SAPA long operated in/around • Small rural village • Active local government (pre-SAPA) • Minority ethnic Atropian; strongly dislike SAPA/support anti-SAPA • Some inter-ethnic friction; majority Persian residents likely resent U.S. • Majority dissatisfied with food, health, and economic conditions. • Shrinking economy, rising unemployment, increasing poverty • Pipeline laborers, farmers, and seasonal agricultural labor • Basic educational/medical available to most; sporadic electricity	***Marjani:*** • Small rural village • Depend on NGO/IGO for essential services (pre-SAPA) • Some residents may support SAPA • Majority Ethnic Persian; clear ethnic tension (pre-SAPA) likely exacerbated by SAPA • Agricultural economy; minimal growth • Small businesses provide necessities • Limited access to schools, medical facilities, and emergency services NGOs medical support diminished under SAPA • Severely restricted information under SAPA	***Marwandi:*** • Small rural village • Active local government • SAPA activity due to Marwandi Pumping Station's importance • Majority ethnic Atropian; strong dislike of SAPA/likely support anti-SAPA activity • Some Persian-Atropian tension • ROA funded school • Primary occupations farmers, rural labor, and pipeline/pumping station workers.

AO	area of operations	OA	operational area
ASR	alternate supply route	ROA	Republic of Atropia
MSR	main supply route	SAPA	South Atropian People's Army
IGO	intergovernmental organization	USAID	United States Agency for International Development
NGO	nongovernmental organization		

Figure 2-1. Example overlay that depicts relevant information about the populace in the area of operations (*continued*)

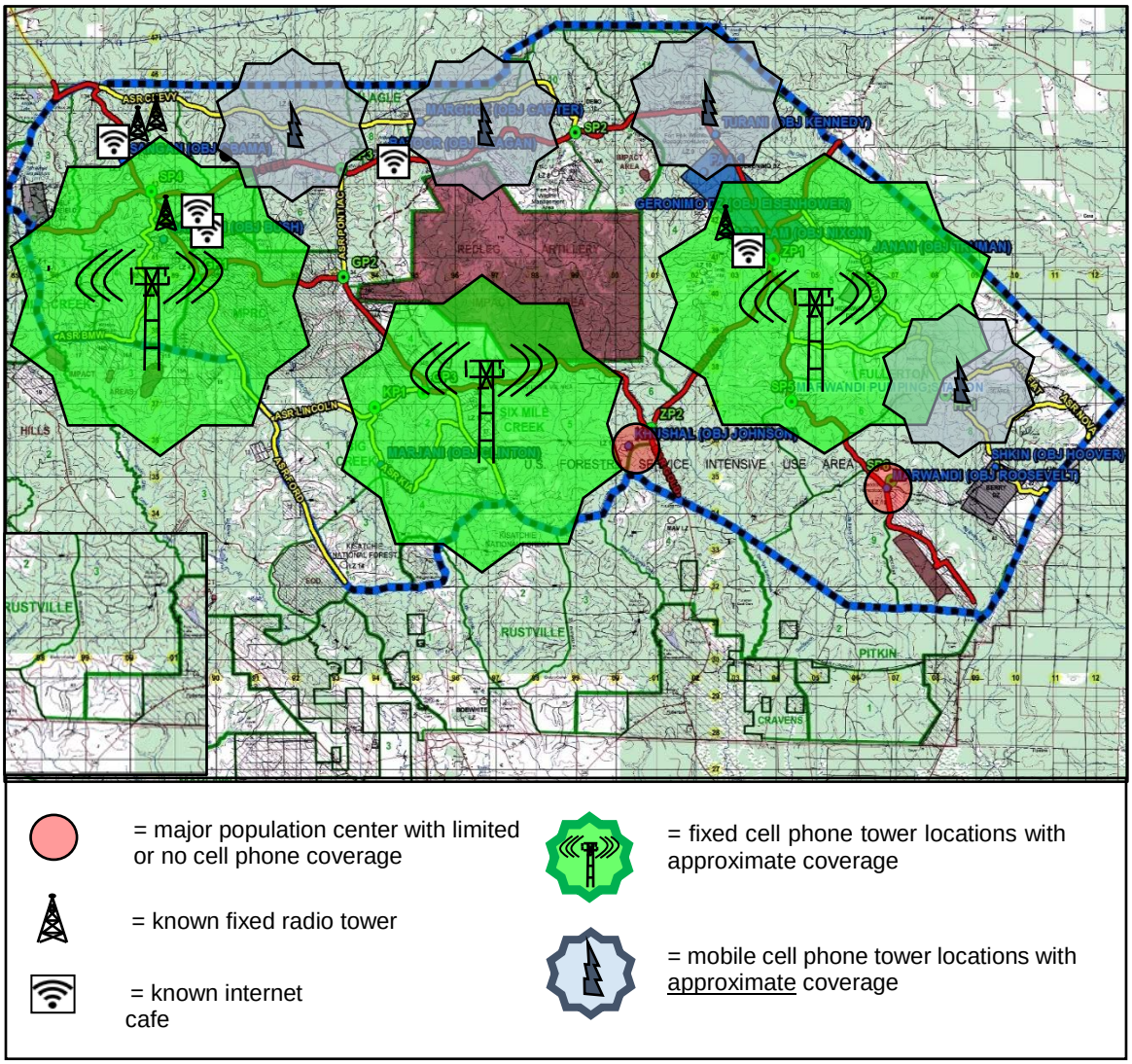

Figure 2-2. Example overlay that depicts relevant information about communications infrastructure in the area of operations

2-27. Next, the IO officer or planner refines the information overlays to produce a "so what" statement for each. Put another way, IO officers iteratively refine information overlays to capture and display those features and impacts that most affect mission accomplishment. The information environment is complex. While oversimplifying it can lead to faulty conclusions and decisions, staffs must competently represent it in a few products that enable commanders to visualize and understand it sufficiently to make informed decisions.

2-28. Once IO planners have generated an information overlay for each significant characteristic, they determine the aggregate impacts across all significant characteristics, mindful of these questions, among others:

- How will each significant characteristic impact the others?
- How does the interaction among significant characteristics impact employing IRCs and the content and flow of information?
- What slow-go or no-go areas in the information environment constrict, restrict, or prevent information flow; what areas facilitate or hasten its flow?

Figure 2-3 illustrates possible impacts among significant characteristics across the three information environment dimensions.

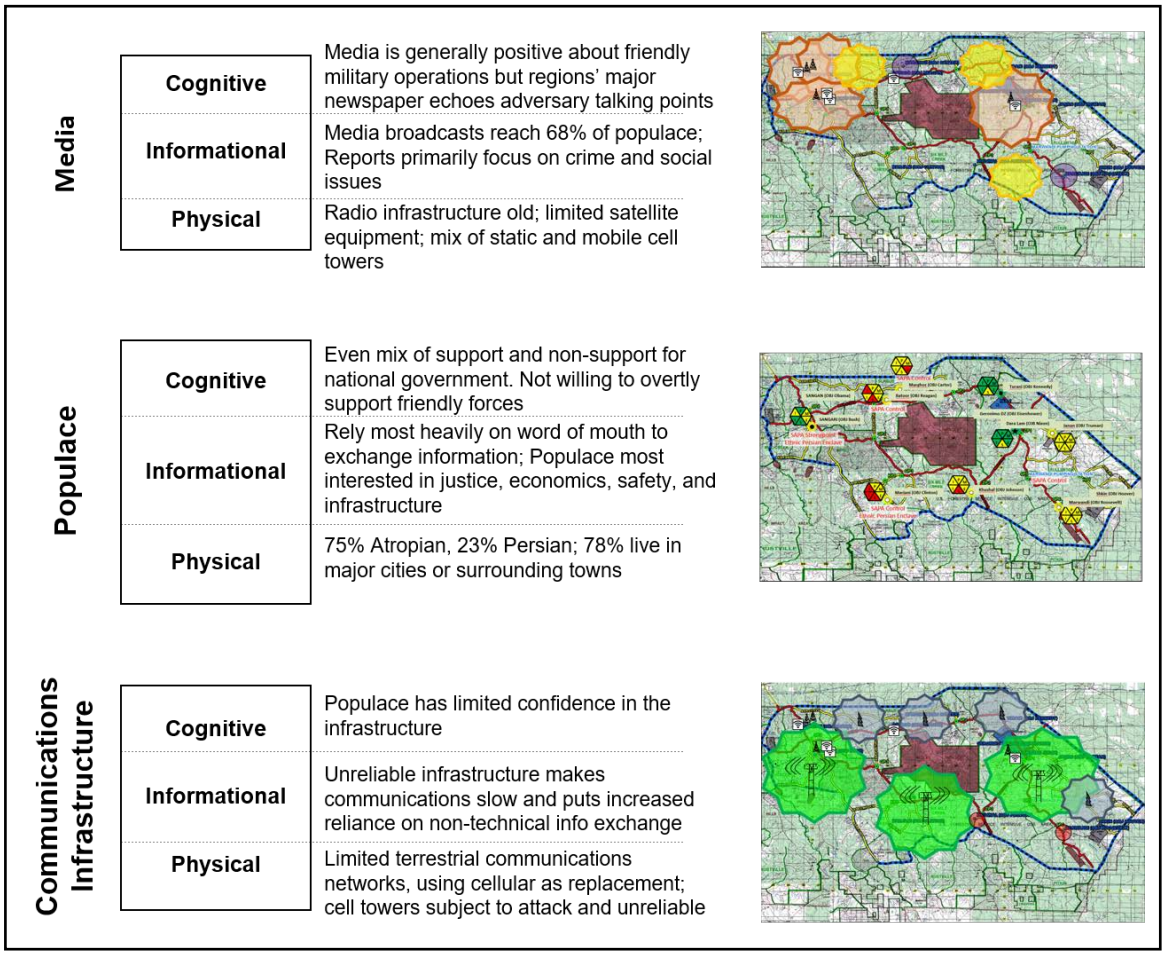

Figure 2-3. Sample description of the information environment effects

STEP 3: EVALUATE THE THREAT'S INFORMATION SITUATION

2-29. Opposing forces use the information environment just as they use the physical domains of air, land, maritime, and space. They aim to gain positions of relative advance, place their enemy at a disadvantage, dominate the information environment, and achieve their objectives. In this step, the staff determines threat capabilities; doctrinal principles; and tactics, techniques, and procedures that threat forces prefer to employ. The IO staff identifies how enemies or adversaries view and use the information environment, including how they array their forces and employ capabilities to create effects in this environment.

2-30. The IO staff applies critical thinking to avoid confirmation bias, groupthink, and other biases. A common mistake is presuming that the adversary views and, therefore, uses the information environment in the same way as U.S. forces—that they are bound by the same constraints or limited by the same means. To avoid mirror-imaging the friendly concept of IO upon the enemy or adversary and prevent mismatching U.S. capabilities and vulnerabilities, the IO staff views adversary operations in the information environment in terms of activities to collect, protect, and project information. These three functions are universal to any armed force's ability to use information as combat power regardless of its organization, capabilities, and mission. As such, these functions form the basis of a threat's capabilities (and vulnerabilities) in the information environment (see table 2-3 on page 2-12 for a description of adversary functions).

Table 2-3. Adversary functions

Term	*Definition*
Collect	To plan and execute operations, the adversary must collect accurate and timely information
Protect	To ensure its ability to make timely and informed decisions, the adversary must protect its critical information from collection and maintain its means of communication
Project	To further its goals and objectives, the adversary must project the information into the information environment to influence the perceptions of its target audiences

2-31. Depending on the threat, the means used can be as simple as direct human observation and open sources (collect); couriers and intimidation (protect); and public broadcasts, printed materials, graffiti, or lethal action. When taken together, these means create a cohesive narrative (project). Ideally, analysis of how the adversary operates in the information environment is based on modeling or templating. Two common tools to conduct this analysis are threat templates and center of gravity (COG) analysis.

2-32. The resulting analysis is an understanding of threat capabilities and vulnerabilities under unconstrained conditions in the information environment. IO planners then refine this understanding using the actual, constrained conditions identified in the information environment analysis and depicted in information overlays and the combined information overlay (for more information on threat templates and center of gravity analysis, see JP 2-01.3 and ATP 5-0.1, respectively).

THREAT TEMPLATES

2-33. Threat templates graphically portray how the threat might use its capabilities to perform the functions required to accomplish its objectives when not constrained by the effects of an operational environment. Threat templates are scaled to depict the threat's disposition and actions for a particular type of operation (for example, offense, defense, insurgent ambush, or terrorist kidnapping). Threat templates are the result of careful analysis of a threat's capability, vulnerabilities, doctrinal principles, and preferred tactics, techniques, and procedures that, in turn, lead to developing threat models and situation templates (see ATP 2-01.3). When possible, IO planners place these threat templates on a terrain product (such as a paper or digital map), adjusting time and distance relationships as necessary, but without violating the threat's fundamental doctrinal precepts. When not practical to overlay these templates on a terrain product, templates nonetheless depict doctrinal interrelationships of threat information warfare forces, key personnel, capabilities, and assets.

2-34. In terms of threat information warfare, threat templates seek to depict doctrinal information usage and flow, decision-making nodes, and locating IRCs, informational systems, sub systems, and associated assets. IO planners typically use three templates:

- Decision-making or information exchange template.
- Information infrastructure template.
- Information tactics template.

2-35. IO planners coordinate with the intelligence staff officer to incorporate information-related threat templates into the threat model. This coordination creates accurate situation templates and subsequent COAs in Step 4 of IPB. Threat templates allow the staff to fuse all relevant combat information and identify intelligence gaps. Further, they enable the staff to predict threat activities—in this case, in the information environment—and adopt COAs, as well as synchronize information collection.

Decision-Making Template

2-36. Also termed an information exchange template, this model considers and then depicts who makes or supports decisions and how they exchange information to support their decision making. It reveals human nodes and links that a threat organization uses to exchange information, with particular emphasis on ways the threat commander receives and disseminates information. Developing this template requires an understanding of threat organizational structures, critical links and interrelationships, and key personnel affecting the decision-making process.

Information Infrastructure Template

2-37. This template considers and then depicts the assets and means the threat employs to exchange information. If the decision-making template focuses on *who* is involved with information exchange, the infrastructure template focuses on *what* enables them to exchange that information. It depicts known infrastructure to exchange information internally and externally. Examples include satellite uplinks or downlinks, radio antennas, cell towers, couriers, and face-to-face interactions.

Information Tactics Template

2-38. The tactics template models how the threat arrays or employs its information assets and capabilities. While the first two templates do not necessarily have to be overlaid on terrain, the tactics template works best depicted as an overlay, so that staffs can clearly see and understand time and distance relationships. Not every adversary will have formal organizations or doctrine for employing information assets and capabilities; thus, the IO officer carefully avoids mirroring U.S. doctrine, capabilities, and methods onto the threat.

THREAT CENTER OF GRAVITY ANALYSIS

2-39. An IO planner uses a COG analysis to identify threat capabilities, requirements, and vulnerabilities. The IO officer does not conduct a separate COG analysis but participates in and contributes to the staff COG effort, led by the intelligence staff officer. The IO officer brings to this effort expertise in the information environment.

2-40. COG analysis, with an emphasis on the information environment, is used to—

- Identify potential threat COGs.
- Identify critical capabilities.
- Identify critical requirements for each critical capability.
- Identify critical vulnerabilities for each critical requirement.
- Prioritize critical vulnerabilities.

Identify Potential Threat Centers of Gravity

2-41. In this step, the staff visualizes the threat as a system of functional components. Based upon how the threat organizes, fights, makes decisions, and uses its physical and psychological strengths and weaknesses, the staff selects the threat's primary source of moral or physical strength, power, and resistance. Depending on the level (strategic, operational, and tactical), COGs may be tangible entities or intangible concepts. To test the validity of the COG, the staff asks: "Is the COG capable of achieving the threat's objective?" The COG is supported, not supporting; if something provides support or contributes to a function that ultimately achieves the threat's objective, then it is a capability or a requirement, not a COG. Typically, a threat COG in the information environment is the threat's information position, which is a way of describing the quality of information the threat possesses and its ability to use that information.

Identify Critical Capabilities

2-42. The IO planner analyzes each COG to determine what primary abilities (functions) the threat possesses in the context of the operational area and friendly mission that can prevent friendly forces from accomplishing the mission. Critical capabilities are not tangible objects; rather, they are threat functions. To test the validity of a critical capability, the staff asks: "Is the identified critical capability a primary ability in context with the given missions of both threat and friendly forces? Is the identified critical capability directly related to the COG?" A critical capability is a crucial enabler for a COG to function and, as such, is essential to accomplishing the adversary's specified or assumed objectives.

Note. The threat's critical capabilities relate to the functions in the information environment—collect, protect, and project.

Identify Critical Requirements for Each Critical Capability

2-43. The IO planner analyzes each critical capability to determine what conditions, resources, or means enable threat functions or mission. To test validity of a critical requirement, the staff asks: "Will an exploitation of the critical vulnerability disable the associated critical requirement? Does the friendly force have the resources to affect the identified critical vulnerability?" If either answer is no, then the IO planner must review the threat's identified critical factors for other critical vulnerabilities or reassess how to attack the previously identified critical vulnerabilities with additional resources.

Note. Critical requirements usually are tangible elements such as communications means, nodes, or key communicators.

Identify Critical Vulnerabilities for Each Critical Requirement

2-44. The IO planner analyzes each critical capability to determine which critical requirements (or components thereof) are vulnerable to neutralization, interdiction, or attack. As a planner develops the hierarchy of critical requirements and critical vulnerabilities, the staff seeks interrelationships and overlapping between the factors to identify critical requirements and critical vulnerabilities that support more than one critical capability. When selecting critical vulnerabilities, a critical-vulnerability analysis is conducted to pair critical vulnerabilities against friendly capabilities.

Note. Critical vulnerabilities may be tangible structures or equipment, or intangible perception, populace belief, or susceptibility.

Prioritize Critical Vulnerabilities

2-45. A tool for prioritizing critical vulnerabilities is CARVER, which stands for criticality, accessibility, recuperability, vulnerability, effect, and recognizability. As a methodology or process, CARVER weighs and ranks six target criteria for targeting and planning decisions. The IO planner applies the six criteria against the critical vulnerability to determine impact on the threat organization as follows:

- **Criticality** is estimating the critical vulnerability's or target's importance to the enemy. Vulnerability will significantly influence the enemy's ability to conduct or support operations. As applied to targeting, criticality means target value and relates to how much a target's destruction, denial, disruption, and damage will impair the enemy or adversary's political, economic, or military operations or how much a target component will disrupt the function of a target complex.
- **Accessibility** is determining whether the critical vulnerability or target is accessible to the friendly force; it is the ease with which a target can be reached.
- **Recuperability** is evaluating how much effort, time, and resources the enemy or adversary must expend if the critical vulnerability or target is successfully affected.
- **Vulnerability** is determining whether the friendly force has the means or capability to affect the critical vulnerability or target using available assets. A target is vulnerable if friendly forces can attack it.
- **Effect** is determining the extent of the effect achieved if the critical vulnerability is successfully exploited. Effect means the impact on the enemy or adversary decision maker or makers. A target should not be attacked unless it can achieve the desired military effect.
- **Recognizability** is determining if the critical vulnerability or target, once selected for an exploitation, can be identified during the operation by the friendly force, and can be assessed for the impact of the exploitation.

2-46. The resulting analysis provides a prioritized list of objectives or targets that can then be discussed in context of each possible COA, aiding COA analysis. Each COA will dictate the capability to be employed (see ATP 3-05.20 for an overview of Army special operations forces targeting methodology that includes COG analysis and CARVER criteria; see ATP 2-33.4 and ATP 3-60 for the Army use of CARVER as a target value analysis tool).

Note. Planners also use COG analysis to identify friendly COGs, capabilities, requirements, and vulnerabilities and CARVER to identify friendly targets that are vulnerable to attack and for defensive purposes.

STEP 4: DETERMINE THREAT COURSES OF ACTION

2-47. Developing a threat COA is a six-step process that requires an understanding of the threat characteristics and the effects of terrain, weather, and civil considerations on operations (see ATP 2-01.3 for a detailed discussion on the threat). These steps include:

- Identify likely objectives and end state.
- Identify the full set of COAs available to the threat.
- Evaluate and prioritize each threat COA.
- Develop each COA in the detail that time allows.
- Identify high-value targets for each COA.
- Identify initial collection requirements for each COA.

2-48. The IO officer or planner filters each step of the process through an information lens, determining possible COAs that rely on the information environment to achieve an advantage. When developing each COA, the IO officer or planner coordinates closely with the intelligence staff officer to ensure each situation template depicts where, when, and why the threat employs its information systems and capabilities. The IO officer or planner develops IO-specific situation templates as a first step in the coordination process. These templates do not stand alone; instead, they contribute to the intelligence staff officer's situation templates. Continual coordination during IPB ensures that the staff develops the most accurate threat COAs.

2-49. While threat templates reflect how the threat should operate based on doctrine or preferred methods, the situation template conveys how the threat actually operates and employs its forces and capabilities based on an operational environment. Figure 2-4 on page 2-16 provides an example information-focused situation template that the IO officer or planner uses to enhance staff coordination during IPB.

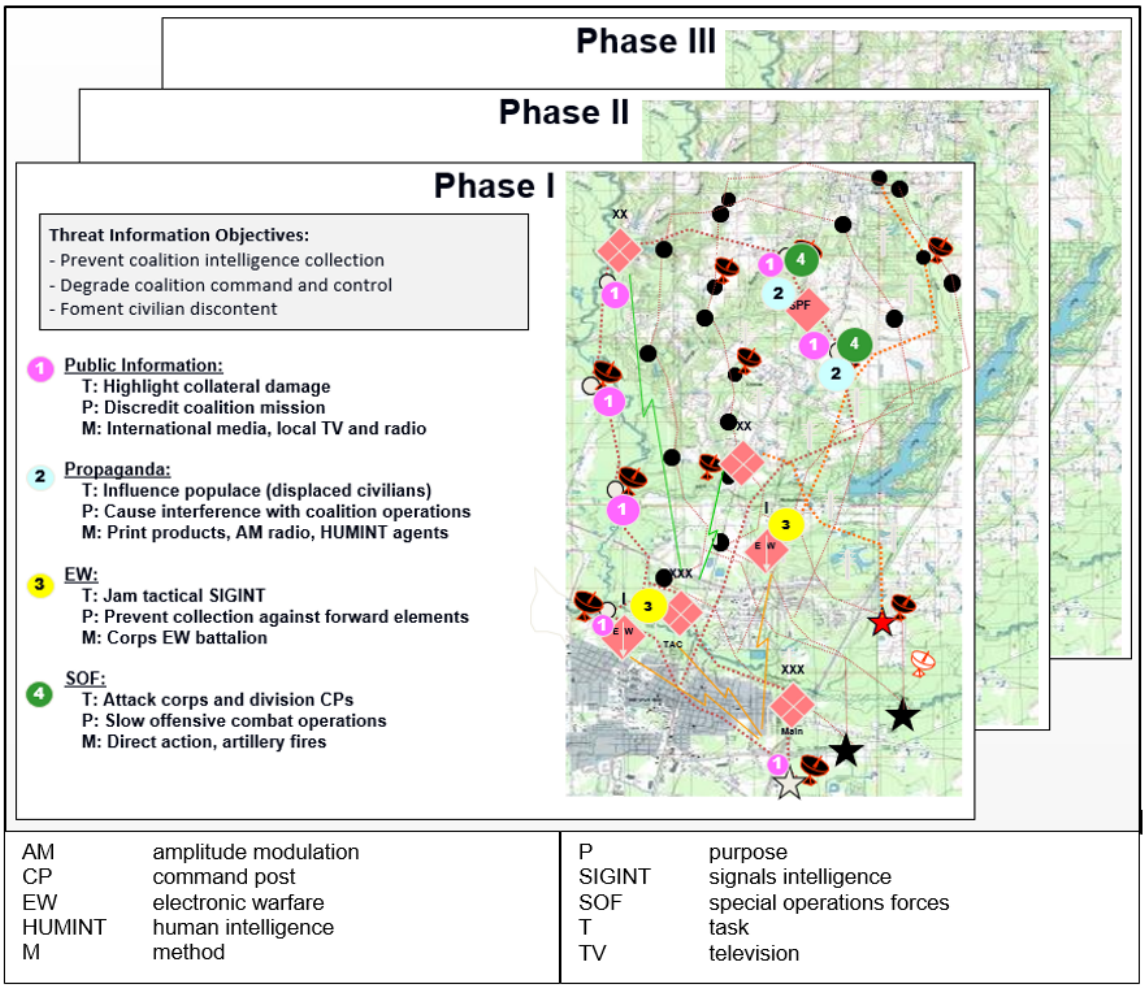

Figure 2-4. Example information situation template

COMBINED INFORMATION OVERLAY

2-50. In addition to the running estimate, IPB to support IO results in producing a graphic visualization product known as the combined information overlay (CIO). The CIO results from the prior analysis conducted in Steps 1 through 4, aggregating the information, threat, and situation templates (or overlays) to depict where and how aspects—such as infrastructure, terrain, and populace—can affect military operations. In certain instances, the IPB may require more than one CIO to capture the full complexity of the information environment.

2-51. The CIO gives the commander and the staff a visual depiction of the ways in which information affects the AO. Similar to the modified combined obstacle overlay, which the intelligence staff officer develops during the IPB, the CIO is a simplified depiction of numerous interconnected variables. The CIO is a tool to visualize a collection of inputs that can never be completely synthesized. As such, it never becomes a final product; it is continually updated as new information arises and as time and staffing permits.

2-52. Reachback capabilities, such as provided by the 1st IO Command, sometimes provide a starting point for a CIO, but the IO working group must verify and refine these products with more localized analysis. The IO officer, aided by the IO working group, is ultimately responsible for the product. Although the CIO may include classified information, particularly when dealing with technical or military aspects of an operational environment or intelligence products, it primarily consists of open-source and publically available

information that is useful once validated. With a request for information, the IO officer can obtain additional information about the threat from the intelligence staff.

Note. Using open-source and publically available information for other than intelligence purposes should not be confused with open-source intelligence (known as OSINT). Only intelligence personnel conduct open-source intelligence (see ATP 2-22.9 for more on this topic).

2-53. Figure 2-5 on page 2-18 illustrates a sample CIO. What appears in or on the CIO depends on the situation, mission, commander preferences, and the resulting analysis. Templates include a combination of narrative (descriptive) elements, pictorial elements, and graphical elements. Whether the "so what" statement appears on the template itself or in accompanying notes, it needs to be conveyed concisely to the commander. The proportion of one element to the others depends on the conclusions the IO officer reaches and a judgement call on the best way to convey these conclusions.

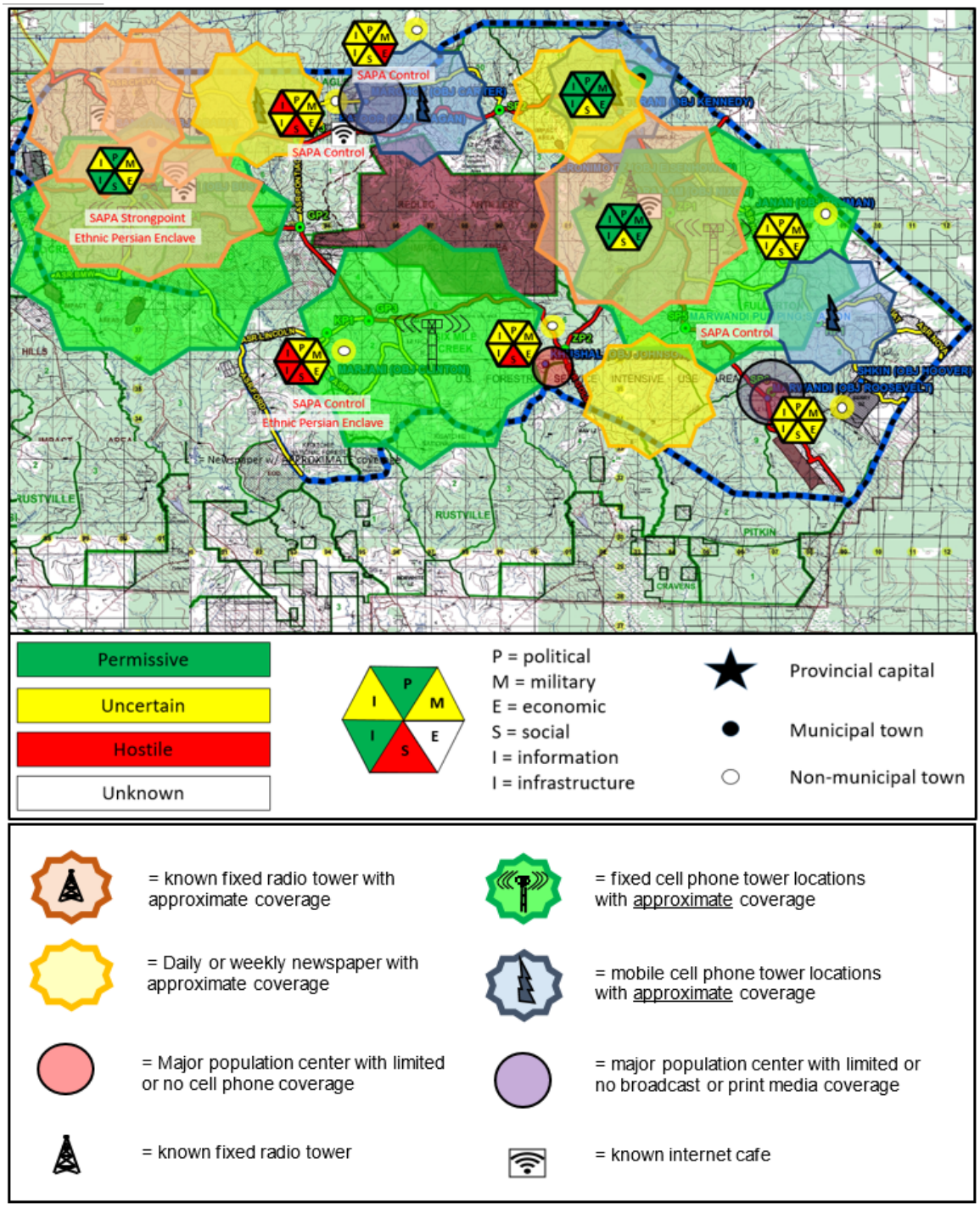

Figure 2-5. Example of combined information overlay

Chapter 3
Information-Related Capabilities

DETERMINATION OF ASSETS

3-1. As a part of mission analysis, the IO officer or representative reviews available assets and identifies resource shortfalls. The IO officer inventories available IRCs, IRCs to request from higher headquarters, and IRCs available through unified action partners. The IO running estimate—paragraph 1.b.(4) "Friendly Forces"—or a suitable block in a graphical estimate reflects the results of the inventory (see the FM 6-0 chapter on running estimates).

3-2. Without accurate accounting for what assets—particularly IRCs—are available, the IO officer cannot effectively formulate schemes of IO during COA development. The scheme of IO is a clear, concise statement of where, when, and how the commander intends to employ and synchronize IRCs to create effects in and through the information environment to achieve the mission and support decisive operations. Based on the commander's planning guidance, the IO officer develops a separate scheme of IO for each COA the staff develops. Schemes of IO are written in terms of IO objectives—and their associated weighted efforts (attack, defend, stabilize)—and IRC tasks required to achieve these objectives (see FM 3-13, Chapter 2, for more information on IO weighted efforts). For example, the overall scheme may be weighted heavily on defending friendly information but also include attack and stabilize objectives (see chapter 4 for more information about schemes of IO).

3-3. IRCs exist at all echelons but are more numerous and diverse at higher levels. Table 3-1 on page 3-2 depicts IRCs by echelon (not in any order of priority). This echeloning is not absolute and varies depending on mission and task organization. As discussed beginning in paragraph 3-4, IRCs are broadly categorized as intrinsic or extrinsic. As JP 3-13 and FM 3-13 make clear, any capability that produces an effect in the information environment is considered an IRC. For example, when units employ fires to create an effect in the information environment (to influence or change behavior), it is an IRC in that instance. Examples of other capabilities that create effects in the information environment include, but are not limited to—

- Commander's communication synchronization.
- Foreign disclosure.
- Knowledge management and information management.
- Military intelligence and counterintelligence.
- Military police engagement.
- Physical security.

CATEGORIES OF INFORMATION-RELATED CAPABILITIES

3-4. Two broad categories of IRCs exist: intrinsic and extrinsic. Intrinsic IRCs are those capabilities internal to or embedded in an Army unit. Extrinsic IRCs are those capabilities that exist outside the unit, such as those available at or through higher or other headquarters or that are joint, interagency, non-governmental, or belong to other unified action partners. Table 3-1 arrays intrinsic and extrinsic IRCs by echelon.

INTRINSIC INFORMATION-RELATED CAPABILITIES

3-5. Intrinsic IRCs are inherent in a unit's mission and table of organization or modified table of organization. They are either leader- or staff-led. As an example, presence, profile, and posture (PPP) is inherent in every unit because it relies on effectively combining decision making, available personnel, and systems to project influence. Similarly, Soldier and leader engagement (SLE) is inherent in every unit.

Operations security is a program and a process that protects friendly information and relies on an assigned staff person to plan and execute it. Similarly, military deception is executed through an assigned staff person.

EXTRINSIC INFORMATION-RELATED CAPABILITIES

3-6. Extrinsic IRCs are external capabilities made available through assignment, attachment, or other command or support relationships for specific times or missions (see FM 6-0, Appendix B, for more information on command and support relationships). The operations of these capabilities are planned and coordinated with the unit to which they have a command or support relationship, but executed by the commander or senior representative of that capability. For example, a brigade combat team is typically supported by both a reserve component civil affairs company and a psychological operations (PSYOP) company. These capabilities often have elements or representatives on the supported unit's staff that provide liaison between them. These capabilities also are characterized by their alignment to a force modernization proponent. For example, the John F. Kennedy Special Warfare Center and School is the proponent for both CAO and MISO.

Table 3-1. Intrinsic and extrinsic information-related capabilities by echelon

Battalion and Below	*Brigade*	*Echelons Above Brigade*	
PPP	PPP	PPP	Intrinsic
PA	PA	PA	
SLE	SLE	SLE	
OPSEC	OPSEC	OPSEC	
CMO	CMO	CMO	
MILDEC	MILDEC	MILDEC	
PR	PR	PR	
Soldier camera	COMCAM	COMCAM	
Physical security	Physical security	Physical security	
Physical maneuver	Physical maneuver	Physical maneuver	
Destruction & lethal action	Destruction & lethal action	Destruction & lethal action	
MISO	MISO	MISO	Extrinsic
CAO	CAO	CAO	
Police engagement	Police engagement	Police engagement	
	EW	EW	
		CO	
		Space operations	
		IJSTO	
		SAP	

CAO	civil affairs operations	MISO	military information support operations
CMO	civil-military operations	OPSEC	operations security
CO	cyberspace operations	PA	public affairs
COMCAM	combat camera	PPP	presence, profile, and posture
EW	electronic warfare	PR	personnel recovery
IJSTO	integrated joint special technical operations	SAP	special access program
MILDEC	military deception	SLE	Soldier and leader engagement

LISTING OF INFORMATION-RELATED CAPABILITIES

3-7. Paragraphs 3-7 through 3-51 provide overviews of each IRC. They are listed alphabetically, in part to reinforce the idea that they are co-equal in their potential contribution to the scheme of IO. Every IRC has one characteristic in common: a representative of each capability is a member of the IO working group. Some are habitual or core members while others attend on an as-needed basis. In either case, their participation is governed by the mission, current situation, and commander's discretion.

CIVIL AFFAIRS OPERATIONS

3-8. CAO encompass actions planned, executed, and assessed by civil affairs forces. These actions—

- Enhance awareness of and manage the interaction with the civil component of an operational environment.
- Identify and mitigate underlying causes of instability in civil society.
- Involve the application of functional specialty skills normally the responsibility of civil government.

Civil affairs forces engage and influence the civil populace and authorities by planning and conducting CAO. These forces enable civil-military operations, shape the civil environment, and set the conditions for military operations.

3-9. The staff focal point for CAO and civil-military operations is the civil affairs staff officer. This officer is a core member of the unit's IO working group (see FM 3-57 for a detailed discussion of civil affairs).

CIVIL-MILITARY OPERATIONS

3-10. Civil-military operations are activities of a commander performed by designated civil affairs or other military forces that establish, maintain, influence, or exploit relations between military forces, indigenous populations, and institutions. Civil-military operations directly support attaining objectives related to reestablishing or maintaining stability in a region or host nation.

3-11. Civil-military operations (known as CMO) activities establish, maintain, influence, or exploit relations among military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area to achieve U.S. objectives. In civil-military operations, personnel perform functions normally provided by the national, regional, or local government, placing them into direct contact with civilian populations. This level of interaction results in civil-military operations significantly affecting the perceptions of the local populace (see JP 3-57 for more information on civil-military operations).

COMBAT CAMERA

3-12. Combat camera (COMCAM) provides operational imagery; supports combat, information, humanitarian, special force intelligence, engineering, legal, and public affairs requirements; provides imagery that supports strategic, operational, and tactical levels of war; speeds decision making; and facilitates the vertical and horizontal flow of information. Further, COMCAM supports information collection, battle damage assessment, military deception, legal, and historical or archival functions. COMCAM units maintain the capability to acquire, edit, disseminate, archive, manage, and transmit imagery. All COMCAM units are equipped to acquire imagery in darkness and inclement weather.

3-13. Normally, COMCAM augments the IO officer or IO elements. If assigned, the COMCAM officer manages all COMCAM assets by planning, preparing, and executing COMCAM activities; if not assigned, the IO officer provides planning and guidance on COMCAM employment. When COMCAM units are unavailable, particularly at battalion and below levels, units can designate one or more Soldiers to use unit-issued or personal cameras (referred to as Soldier camera); however, the unit must have a procedure in place for the review, clearance, and disposition of any images taken (see ATP 6-02.40).

CYBERSPACE ELECTROMAGNETIC ACTIVITIES

3-14. *Cyberspace electromagnetic activities* is the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations (ADRP 3-0). Cyberspace electromagnetic activities (CEMA) is, therefore, not an IRC in and of itself; cyberspace operations and EW operations are IRCs. Through CEMA, the Army plans, integrates, and synchronizes these missions, supports and enables the mission command system, and provides an interrelated capability for information and intelligence operations. CEMA also plays a significant role in attacking enemy or adversary decision making, while protecting friendly forces. The continuous planning, integration, and synchronization of cyberspace operations and EW, enabled by spectrum management operations, can produce singular, reinforcing, and

complementary effects. Cyberspace operations and EW both operate using the electromagnetic spectrum. *Spectrum management operations* is the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations (FM 6-02).

3-15. The staff focal point for CEMA at and below the division level is the EW officer, who has additional responsibility as the cyberspace planner. The EW officer serves as the commander's designated staff officer for planning, integrating, synchronizing, and assessing cyberspace operations and EW. This officer is typically a core member of the unit's IO working group (see FM 3-12 for a discussion of CEMA).

Electronic Warfare

3-16. *Electronic warfare* is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). EW capabilities enable Army forces to create conditions and effects in the electromagnetic spectrum to support the commander's intent and concept of operations. EW includes electronic attack, electronic protection, and electronic warfare support, and includes activities such as electromagnetic jamming, electromagnetic hardening, and signal detection, respectively. EW affects, supports, enables, protects, or collects on capabilities operating within the electromagnetic spectrum, including cyberspace capabilities. With proper integration and deconfliction, EW can create reinforcing and complementary effects by affecting devices that operate in and through wired and wireless networks.

Cyberspace Operations

3-17. *Cyberspace operations* are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0). Army cyberspace operations range from defensive to offensive, establish and maintain secure communications, and detect and deter threats in cyberspace to the Department of Defense information network as they support Army and joint forces from strategic to tactical levels.

INTEGRATED JOINT SPECIAL TECHNICAL OPERATIONS AND SPECIAL ACCESS PROGRAMS

3-18. Integrated joint special technical operations (IJSTO) are classified operations that harness specialized technical capabilities to gain a decisive advantage over an enemy or adversary. These technical capabilities can be information-related or, in some way, complement IO efforts. Therefore, IJSTO and IO must be deconflicted and synchronized through close coordination, primarily through the IO working group. According to JP 3-13, detailed information about IJSTO and its contribution to IO can be obtained from IJSTO planners at combatant command or Service component headquarters.

3-19. Special access programs (known as SAPs) are sensitive acquisition, intelligence, or operations and support programs that impose need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information (see DODD 5205.07 for more information on special access programs). As with IJSTO, detailed information related to special access programs can be obtained, when authorized, from the designated representative at combatant command or Service component headquarters.

MILITARY DECEPTION

3-20. Military deception (MILDEC) involves actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers. The intent of MILDEC is to feed information that deliberately misleads the enemy decision makers as to friendly military capabilities, intentions, and operations and lead the enemy to take actions (or inactions) that contribute to accomplishment of the friendly mission. When properly integrated with operations security, other IRCs, and visible activities of the joint force and its components, MILDEC can be a decisive tool in altering how the adversary views, analyzes, decides, and acts in response to friendly military operations.

3-21. MILDEC is both a process and a capability. As a process, MILDEC is a methodical, information-based strategy that systematically, deliberately, and cognitively targets individual decision makers. The objective

is the purposeful manipulation of decision making. As a capability, MILDEC is useful to a commander when integrated early in the planning process as a component of the operation focused on causing an enemy to act or react in a desired manner.

3-22. MILDEC is accomplished various ways. Chief among these ways are tactical deception, counterdeception, and deception to support operations security.

3-23. Tactical deception consists of deception activities planned and conducted to support battles and engagements in real time. Tactical-level commanders plan and execute tactical deception to cause enemy actions favorable to U.S. objectives. These activities aim to gain a tactical advantage over an adversary, to mask vulnerabilities in friendly forces, or to enhance the defensive capabilities of friendly forces.

3-24. Counterdeception contributes to situational understanding by protecting friendly human and automated decision making from adversary deception. Counterdeception strives to make Army commanders aware of adversary deception activities so they can formulate informed and coordinated responses.

3-25. The goal of deception to support operations security is to help protect friendly operations, personnel, programs, equipment, and other assets against foreign intelligence entities, insurgents, and adversarial collection. It creates multiple false indicators to confuse the enemy or adversary. Sometimes they make friendly intentions harder for the enemy or adversary intelligence gathering apparatus to interpret or limit the enemy's ability to collect accurate information on friendly forces.

3-26. The staff focal point for deception is the assigned or designated MILDEC officer, who should be part of the operations staff section in the IO element. The MILDEC officer is a core member of the IO working group (see JP 3-13.4 for a detailed discussion on MILDEC).

MILITARY INFORMATION SUPPORT OPERATIONS

3-27. *Military information support operations* 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 in a manner favorable to the originator's objectives (JP 3-13.2). PSYOP forces conduct three distinct missions: military information (known as MILINFO), interagency-intergovernmental support (known as IIS), and civil authority information support (known as CAIS). Military information is the only mission relevant to IO planning.

3-28. Military information consists of psychological actions and persuasive messages executed during military operations to influence selected individuals and groups in ways that support U.S. national objectives. At the tactical level, PSYOP forces execute actions (or coordinate their execution) and deliver audio, visual, and audio-visual messages that encourage enemy forces to defect, desert, flee, surrender, or take any other action beneficial to friendly forces.

3-29. At brigade and above, the focal point is the staff PSYOP officer or noncommissioned officer, in close coordination with the IO officer or representative. Additionally, the commander or officer-in-charge of an attached PSYOP unit may also contribute to synchronizing IRC. Both individuals are core members of the unit's IO working group.

OPERATIONS SECURITY

3-30. *Operations security* is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities (JP 3-13.3). The operations security (OPSEC) process meets operational needs by mitigating risks associated with vulnerabilities to deny the threat critical information and observable indicators. A successfully executed OPSEC program enables operations by preventing misinformation, disinformation, and information fratricide.

3-31. OPSEC aims to enhance the probability of mission success by preserving the advantages of essential secrecy and surprise. Commanders use OPSEC measures to deny the threat knowledge of friendly operations, requiring the threat to expend more resources to obtain critical information needed to make decisions. OPSEC is a force multiplier. It includes—

- Reducing predictability.
- Eliminating indicators of operations.
- Disrupting the adversary's information gathering.
- Preventing the adversary's recognition of indicators by using diversions, camouflage, jamming, and deterrence.
- Preventing counteranalysis, which seeks to prevent accurate interpretations of indicators during adversary analysis of collected material.

Once staffs identify vulnerabilities, they can use other IRCs such as MILDEC to satisfy OPSEC requirements. OPSEC practices must balance the responsibility to account to the American public with the need to protect critical information. OPSEC should not be used as an excuse to deny noncritical information to the public.

3-32. The focal point for OPSEC is the designated OPSEC planner. This individual is typically co-located with the IO officer or representative as part of the IO element (see JP 3-13.3 and AR 530-1 for details on OPSEC).

PERSONNEL RECOVERY

3-33. The core principle of Army personnel recovery (PR) is to recover isolated personnel before detention or capture through a systems-based approach that features proactive, integrated, rehearsed, and resourced measures and capabilities. To fulfill this principle, the Army has an obligation to train, equip, and protect its personnel (Soldier, DA Civilian, and contractor), prevent their capture and exploitation by adversaries, and reduce the potential for using isolated personnel as leverage against U.S. security objectives and national interests. The IO officer works with the personnel recovery officer to—

- Reduce interference between U.S. and coalition PR operations.
- Decrease the effectiveness of hostile propaganda and misinformation because of captured or detained personnel
- Increase support and cooperation from unified action partners for PR operations.
- Integrate PR considerations into MISO, deception, and public affairs plans.
- Synchronize and coordinate IO in the overall operation to mislead the enemy about recovery operations and assets.

Note. PR did not appear in FM 3-13, 1 Dec 2017, but is added here, reinforcing the fact that any capability can serve as an IRC if it is affected by or affects the information environment.

PHYSICAL ATTACK

3-34. When synchronized as a part of information operations, physical attack—which includes physical maneuver, destruction, and lethal action—is the application of combat power to create desired effects in the information environment. Carefully applied force can play a major role in intimidation and deterrence and in obstructing a threat's ability to exercise command and control. It may include direct and indirect fires from ground, sea, and air platforms and direct actions by special operations forces. IO applications of physical attack to consider include—

- Preventing or degrading adversary reconnaissance and surveillance.
- Conducting physical attacks as deception events.
- Degrading the enemy's ability to process information.
- Degrading the enemy's ability to jam communications.
- Destroying command and control and communications systems.
- Reducing the enemy's ability to penetrate mission command systems.

As the list reveals, physical attack typically supports or complements other capabilities such as military deception, electronic warfare, or cyberspace operations.

3-35. When applying physical attack as a component of IO, consideration of second- and third-order effects, as well as consequence management, is a must. Total, or even partial, destruction of threat systems or

capabilities or of indigenous capabilities co-opted by an enemy or adversary, may not be attainable or even desirable. For example, friendly forces may need to use threat command and control systems during the postconflict phase of military operations. Additionally, destructing indigenous capabilities may create animosity among the local populace, the effects of which are greater than any advantage gained over the threat.

PHYSICAL SECURITY

3-36. *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 (JP 3-0). Physical security contributes directly to IO and each of its weighted efforts, most especially efforts to defend personnel, information, and systems that contribute to friendly decision making. Information, information-based processes, and information systems—such as mission command systems, weapon systems, and information infrastructures—are protected relative to the value of the information they contain and the risks associated with the compromise or loss of information.

3-37. Physical security is a unit program directed by the commander and overseen by the operations staff officer (see AR 190-13 and AR 190-16 for details on physical security).

PRESENCE, PROFILE, AND POSTURE

3-38. The mere presence of a force can significantly affect all audiences in the AO. Deploying, moving, or assigning forces to the right place at the right time can add substantial credibility to messages being delivered through other channels and provide a major contribution to deterrence. Whenever Soldiers or forces leave base or cross the line of departure, they do two things: collect information and send a message. If either collection or PPP are not a deliberate, coordinated effort, both the information coming back and the message sent appear haphazard and inconsistent. PPP is always in play, and the IO officer should always provide PPP guidance on behalf of the commander.

3-39. Presence is the act of being physically present, although technology is increasingly enabling virtual presence. Presence can be menacing or reassuring, depending on the situation. Absence, or the lack of presence, can create perceptions that work for or against the unit's aims. Being very conscious and deliberate about being present or absent can be a powerful form of influence and should not be left to chance. Once units determine presence is required, or no choice exists but to be present, how they convey that presence is important. Both profile and posture address the way units, patrols, and Soldiers are present.

3-40. Profile is about the degree of presence, both in terms of quantity and quality. Quantity is reflected in how much a unit is present, as in its footprint or task organization. Quality speaks to the nature of that presence, as in its current capability, as well as its reputation.

3-41. The posture of a unit is an expression of its attitude. Whether active or passive, threatening or non-threatening, defensive or welcoming, posture dictates how units or Soldiers appear to others and how Soldiers act towards others. For example, the decision to wear soft caps instead of Kevlar helmets and body armor can considerably affect the perceptions and actions of adversaries and the local populace.

3-42. The operations officer and IO officer or representative are the focal points for PPP. All leaders and Soldiers contribute to it.

PUBLIC AFFAIRS

3-43. Army *public affairs* is communication activities with external and internal audiences (JP 3-61). Public affairs operations help to establish conditions that lead to confidence in the Army and its readiness to conduct unified land operations. It supports the commander's responsibility to keep the American people and the Army informed.

3-44. Public affairs personnel direct their efforts using public information, command information, and community engagement. Public information focuses on informing external audiences. It primarily engages the media and key audiences to convey Army and command themes and messages to American and global

audiences. Command information focuses on internal audiences—Soldiers, DA Civilians, and Family members. Commanders recognize that an informed force is a more ready, reliable, and resilient force. Community engagement focuses on working collaboratively with, and through, groups of people affiliated by a geographic proximity or special interest to enhance the understanding and support for the Army, Soldiers, operations, and activities. It recognizes that a positive rapport between the Army and its host communities is mutually beneficial, supporting the Army as an institution as well as its individual Soldiers.

3-45. The public affairs officer or designated representative is the commander's personal advisor on public affairs matters. The public affairs officer or representative is the focal point for public affairs integration into the operations process and determines the appropriate public affairs posture for a given operation. Close coordination with the IO officer or representative is essential to ensure effects of an IRC are optimized and deconflicted with public affairs and the public affairs posture is supported during SLEs or other engagements; as such, the public affairs officer is a core member of the IO working group (see FM 3-61).

SOLDIER AND LEADER ENGAGEMENT

3-46. *Soldier and leader engagement* is defined as interpersonal Service-member interactions with audiences in an area of operations (FM 3-13). These interactions can be dynamic, such as an impromptu meeting on the street or deliberate, such as a scheduled meeting. SLE can be in-person and face-to-face or conducted at a distance, facilitated by technology.

3-47. A primary purpose of SLE is to convey approved, pre-developed messages (to support approved public affairs or MISO themes) to enhance the credibility of unit personnel and legitimacy of unit operations. Key leader engagement is a subset of SLE.

3-48. The commander is the unit's chief engager and designates a staff focal point for planning, synchronizing, and assessing SLE, whether conducted by unit personnel or other IRCs, such as civil affairs, engineering, or military police forces; chaplains or religious affairs personnel; or medical personnel.

3-49. Chaplains and religious affairs personnel conduct SLEs at the commander's direction as the commander's principle advisor on religion, ethics, morals, and morale while maintaining their noncombatant status (see ATP 1-05.03 for details on religious support). By virtue of their roles as religious leaders, chaplains' very presence in an operational area opens avenues of approach for partnership.

POLICE ENGAGEMENT

3-50. Police engagement occurs in all operational environments in which military police interact with elements external to their own organization. Police engagement is an IRC that occurs among police personnel, organizations, and populations for the purpose of maintaining social order. Military police and U.S. Army Criminal Investigative Command personnel engage local, host-nation, and coalition police partners; police agencies; civil leaders; and local populations for critical police information that can influence military operations or destabilize an AO. Ultimately police engagement aims to develop a routine and reliable interpersonal network through which police information can flow to military police. Based on the tactical situation, police engagement can be formal or informal. Police engagement may be a proactive activity as part of deliberate information gathering, targeting, or collection, or it can be conducted as a reactive response to an episodic event (see FM 3-39 for military police operations).

SPACE OPERATIONS

3-51. Space operations are operations that occur in the space domain and seek to gain superiority over enemies and adversaries in the space domain and its corresponding environment. Army space operations include all aspects of employing specialized Army space forces as well as activities associated with the planning, preparation, integration, and execution required to ensure synchronized and effective space-based capabilities from all sources. Space-based capabilities increasingly facilitate the flow of information and decision making. Space control, one mission area of space operations, can be used to deny communications and propaganda tools, such as satellite television and satellite radio, to enemy leadership. Space surveillance systems monitor the status of enemy and commercial satellite operations to determine potential threats to friendly forces (see FM 3-14 for details on space operations).

SOCIAL MEDIA

3-52. The information environment spotlights the growing impact of social media (see also paragraph 2-14). Although not listed in Table 3-1 because it is still an emergent IRC, social media has the potential to become a powerful capability for IO. Some possible applications include—

- Social media as a media channel, such as radio, newspapers, and television.
- Social media as an interactive medium for exerting influence.
- Social media as a means to communicate with an established network or networks.
- Social media as a near real-time sensor-to-sensor network.

3-53. Social media is rapidly expanding beyond the realm of public affairs, IO, or intelligence functions and becoming an integral component of operations, particularly those occurring in and through the information environment. Even as the institutional Army explores force modernization aspects of social media—such as doctrine, organizations, personnel, and training— commanders and staffs need to understand social media's impact and incorporate this understanding into planning and operations (see *Social Media-The Vital Ground: Can We Hold It?* for a broader discussion of social media).

REQUESTING CAPABILITIES NOT ON HAND

3-54. Effective IO officers or representatives complete prior planning to ensure that required nonorganic capabilities are available to units at the right time and place to support IO effects-generation. The lead time necessary to submit requests varies by echelon and the location of the capability being requested.

3-55. For training support, requests for reserve forces often require six months or more advance notice and must be requested through Army and joint training information management systems. The Army Training Information Management System is the system used by U.S. Army Forces Command and the U.S. Army Civil Affairs and Psychological Operations Command to validate requests and plan support. Required support from nonorganic capabilities, such as field support teams from the 1st IO Command (Land) and TIOGs, should be identified at receipt of mission and invited to all planning conferences through formal means.

3-56. For operational support at lower levels, units submit requests for capabilities or requests for forces. Staffs complete a request for capabilities when units can use the capability remotely while completing a request for forces when units need assets to move into theater. For nontheater assets, the request for forces process is the chief means to request necessary augmentation. The IO officer, working with the operations staff officer, articulates and justifies the need and then submits the request through channels for validation and sourcing, typically through a sourcing conference or other mechanism. Once the requests for capabilities or requests for forces are generated by the combatant commander, the next step is the review and approval process. Once the mission is approved through the review and approval process, the Secretary of Defense directs the Joint Staff to issue an execute order (known as EXORD) directing the provider to use its capability in support.

3-57. IO staffs integrate IRCs used to create effects against an enemy or adversary through targeting. Requesting assets through the joint targeting cycle requires target development and joint certification (for more information on target development and targeting tasks, see ATP 3-60).

This page intentionally left blank.

Chapter 4
Synchronization of Information-Related Capabilities

SYNCHRONIZATION COMPONENTS

4-1. Creating effects in the information environment is not random. Units synchronize and sequence IRCs so that they actively contribute to fulfilling the unit's mission in accordance with the commander's intent and concept of operations. Mission command places responsibility for IRC synchronization on the staff; however, without the commander's direct involvement, stated intent, guidance, concept of operations, and narrative, the staff will fail to achieve desired and required operational outcomes.

COMMANDERS' RESPONSIBILITIES

4-2. Commanders drive the conduct of IO and are their unit's key informers and influencers. Their influence is a function of their position, authority, decisions, personal actions, and the combat power their unit generates. Every action they take, operation they lead, capability they employ, and word or image they convey sends a message. Ultimately, they have the responsibility to align and combine each message into a comprehensive and compelling narrative while ensuring their unit fulfills this narrative. Their narrative explains the *why* of military operations.

Note. Commanders ensure all members of the Army Profession live by, adhere to, and uphold the moral principles of the Army Ethic, starting with themselves. As trusted Army professionals, commanders set the example and demonstrate character, competence, and commitment. They strive to consistently make right decisions and take right actions that are ethical, effective, and efficient. The Army Ethic is essential to the conduct of IO, as it ensures actions, words, and images are aligned and mutually reinforcing, thereby enhancing credibility and trust.

4-3. The *why* of operations comes down to establishing credibility and legitimacy. No matter the unit's mission, credibility and legitimacy are essential to success. Both credibility and legitimacy build on the Army bedrock of trust. Credible units match or align their actions with their messages (words and images). Trusted Army leaders and units fulfill commitments, are consistent in what they do, and ensure follow through. Legitimacy maintains legal and moral authority in the conduct of operations. Legitimacy, which can be a decisive factor in operations, is based on the actual and perceived legality, morality, and rightness of the actions from interested audiences' point of view. These audiences include American national leadership and domestic audiences; foreign governments, leaders, and civilian populations in the operational area; threats and adversaries; and other nations and organizations around the world.

4-4. Commanders (and subordinate leaders) are responsible for driving the conduct of IO through their narrative, stated intent, guidance, concept of operations, and risk assessment to achieve desired and required operational outcomes.

COMMANDER'S NARRATIVE

4-5. Aligned and synchronized actions and messages help create and convey a credible narrative comprising legitimate actions. To build trust, enable unity of effort, and strengthen legitimacy, commanders, leaders, and IO professionals demonstrate their character, competence, and commitment through their decisions and actions.

4-6. A *narrative* is an overarching expression of context and desired results (JDN 2-13). It focuses primarily on shaping perceptions of relevant audiences in the AO. Not only does it provide rationale to audiences

affected by military operations but the narrative serves as a guide to units so that their actions (deeds), words, and images appropriately align. The final result: a unit whose actions support and reinforce the narrative and ensure its consistency, viability, and effectiveness.

4-7. The IO officer plays a significant role in assisting the commander to craft the narrative. As the unit's effects coordinator for IRCs, the IO officer advises the commander on ways IRCs can affect operations and ways operations can affect the information and operational environments. An effective narrative helps shape both environments by creating or facilitating conditions favorable to the commander's intent, especially in bolstering confidence in the U.S.'s or coalition's mission and creating an alternative to the enemy's or adversary's narrative.

4-8. Commanders typically develop formal, explicit narratives at the strategic and possibly operational levels and convey them downward, within which subordinate units nest their messages, actions, and activities. Yet even the lowest-level commanders or leaders consciously envision how their units' actions, words, and images either support or confound the approved narrative. These leaders then tailor and adapt unit actions and messages to their AOs. If necessary, subordinate commanders get clarification from higher headquarters (for more information on narratives, see the list of recommended readings in the references).

COMMANDER'S INTENT

4-9. *Commander's intent* is a clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned (JP 3-0). Mission command requires commanders to convey a clear commander's intent for operations in which multiple operational and mission variables interact with the lethal application of ground combat power. Such dynamic interactions—many of which occur in the information environment—often compel subordinate commanders to make difficult decisions in unforeseen circumstances. Commander's intent is also essential for exercising disciplined initiative, which is particularly critical to executing a range of IO actions and activities. Such actions and activities can include military deception, SLE, and PPP.

COMMANDER'S INITIAL AND SUBSEQUENT GUIDANCE

4-10. Commander's planning guidance conveys the essence of the commander's visualization and may be broad or detailed. It outlines an *operational approach*—a broad description of the mission, operational concepts, tasks, and actions required to accomplish the mission (JP 5-0) and discusses COAs the commander initially favors from those the staff should not consider. It broadly describes when, where, and how the commander intends to employ combat power to accomplish the mission within the higher commander's intent. In terms of IO, if commanders determine that an information-related line of effort is decisive or that attaining an IO objective requires a significant lead time, they will issue relevant instructions as part of their guidance. In this guidance, they may frame their narrative and subordinating themes and messages, request information about the information environment, identify key leaders with whom they must engage, and discuss how IRCs will support COAs.

CONCEPT OF OPERATIONS

4-11. The concept of operations describes how the commander or leader envisions an operation unfolding from its start to its conclusion or end state. It determines how accomplishing each task leads to executing the next. It identifies the best ways to use available terrain (both physical and virtual) and employs unit strengths against enemy weaknesses. As a line of effort that supports the overall operation—as well as specific lines of operation or effort—IO is an essential element of any concept of operations. IO's contribution to the concept of operation is expressed in its scheme of IO (see paragraph 4-34 for more information on scheme of IO).

RISK ASSESSMENT

4-12. Commanders and their staffs, as trusted Army professionals, incorporate ethical risk assessments in their planning and conduct of operations. These assessments seek to—

- Mitigate unnecessary risk to personnel and mission accomplishment, friendly and allied forces, and noncombatants.
- Avoid improper use of resources and assets.
- Avert decisions and actions that may produce short-term tactical benefits to operations but long-term negative strategic consequences.

STAFF RESPONSIBILITIES

4-13. The staff has responsibility for conducting IO through synchronizing IRCs. As the staff lead for IO, the IO officer or designated representative develops a range of products and chairs the IO working group. The IO working group is the primary mechanism for synchronization and produces several outputs that drive the unit's efforts in the information environment. These outputs include the IO running estimate; the logic of the effort, commander's critical information requirements and essential elements of friendly information, IO input to base orders and plans, IO synchronization matrix, battle drills, and other products as needed.

INFORMATION OPERATIONS WORKING GROUP

4-14. The IO working group has a purpose, agenda and proposed timing, inputs and outputs, and structure and participants. Figure 4-1 on page 4-4 illustrates these components. To enhance the IO working group's effectiveness, the IO officer and element (if one exists) consider a number of best practices before, during, and after the meeting. Because it relies on information from the commander's daily update briefing and feeds the targeting process, the IO working group occurs between the two events in the unit's battle rhythm (see FM 3-13 for an extended discussion of the IO working group).

4-15. Before the IO working group convenes, the IO officer prepares and disseminates the agenda. Typically, the agenda is pre-set and the same template used at every meeting. However, effective IO officers send the agenda out as a reminder to participants and to give advance notice of possible changes. Additionally, before the meeting, the IO officer ensures that all inputs are up-to-date and shared, if possible.

4-16. Efficient IO officers start on time, keep the meeting on the agenda and running time (typically an hour or less), employ a designated note taker, and summarize key points and due outs before the meeting adjourns. Most importantly, IO officers tie critical discussions, outcomes, and decisions back to the commander's narrative, intent, concept of operations, and guidance.

4-17. Post meeting, the IO officer disseminates the meeting minutes, follows up on due outs, and updates the commander and other unit leaders on key outcomes and outputs. The IO officer also finalizes target nominations in advance of the next targeting meeting.

INFORMATION OPERATIONS RUNNING ESTIMATE

4-18. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (ADP 5-0). Running estimates help the IO officer record and track pertinent information about the information environment leading to a basis for recommendations to the commander.

4-19. The IO officer uses the running estimate to assist with completion of each step of the MDMP. An effective running estimate is as comprehensive as possible within the time available but also organized so that the information is easily communicated and processed. Normally, the running estimate provides enough information to draft the applicable IO sections of warning orders as required during planning and, ultimately, to draft applicable IO sections of the operation order or operation plan.

Purpose	*Agenda and Proposed Timing*	
Prioritize, request, and synchronize IRCs and IO augmentation to optimize effects in and through the information environment. **Battle rhythm**: Before targeting working group	Part 1: Operations and intelligence update	30 min
	• Intelligence update	5 min
	• Information environment update	3 min
	• Operations update or significant activities	7 min
	• Review plans, future operations, and current operations	5 min
	• Assessment update (information requirements, indicators)	5 min
	• Calendar update, due outs, and responsibilities from previous meeting	5 min
	Part 2: Stabilize efforts, if any Part 3: Defend efforts Part 4: Attack efforts } • Review and update synchronization matrix • Guidance and comments	6 min 12 min 12 min

Inputs and Outputs		*Structure and Participants*
Inputs: • Higher headquarters orders and guidance • Commander's intent, concept of operations, and narrative • IRC status (running estimates) • Intelligence collections assets • CIO and IPB • Media monitoring analysis • Cultural calendar • Engagements schedule • Audience analysis • Scheme of IO and synchronization matrix • Commander's objectives for IO • Measures of effectiveness and performance	**Outputs:** • Updated scheme of IO • Updated IO synchronization matrix • Key leader engagement recommendations • Refined themes and messages • Refined operational products • Target nominations • Updated CIO • Plans and orders update • Information requirements	**Lead:** IO officer or representative [Chair: G-3 (S-3), executive officer, deputy commanding officer, or commander] **Core participants:** MISO, G-2 (S-2), subordinate unit representatives, G-3 (S-3), fires, G-9 (S-9), operations security, public affairs, CEMA (CO and EW) **Other participants (mission and situation dependent):** G-1 (S-1), G-4 (S-4), G-5 (S-5), G-6 (S-6), space operations, MILDEC, combat camera, FAO, FDO, special forces liaison, KM officer, engineer, STO chief, chaplain, staff judge advocate, unified action partner representatives

CEMA	cyberspace electromagnetic activities	IPB	intelligence preparation of the battlefield
CIO	combined information overlay	IRC	information-related capability
CO	cyberspace operations	KM	knowledge management
EW	electronic warfare	MILDEC	military deception
FAO	foreign area officer	min	minute
FDO	foreign disclosure officer	MISO	military information support operations
G-1	assistant chief of staff, personnel	S-1	personnel staff officer
G-2	assistant chief of staff, intelligence	S-2	intelligence staff officer
G-3	assistant chief of staff, operations	S-3	operations staff officer
G-4	assistant chief of staff, logistics	S-4	logistics staff officer
G-5	assistant chief of staff, plans	S-5	plans staff officer
G-6	assistant chief of staff, signal	S-6	signal staff officer
G-9	assistant chief of staff, civil affairs operations	S-9	civil affairs operations staff officer
IO	information operations	STO	special technical operations

Figure 4-1. Components of an information operations working group

4-20. Running estimates enable planning officers to track and record pertinent information and provide recommendations to commanders. A generic written format of a running estimate contains six general considerations: situation, mission, course of action, analysis, comparison, and recommendation (see FM 6-0 for a detailed discussion on running estimates). Figure 4-2 provides an IO-specific version of the generic

written format. Variations on this format, such as the example provided in Figure 4-3 on page 4-6, enable the IO officer to spotlight facts and assumptions, critical planning factors, and available forces. The latter of these requires input from assigned or available IRCs. The graphic format also offers a clear, concise mechanism for the IO officer to articulate recommended high-payoff targets, commander's critical information requirements, and requests for forces. Maintaining both formats simultaneously provides certain benefits: the narrative format enables the IO officer to cut-and-paste sections directly into applicable sections of orders; the graphic format enables the IO officer to brief the commander and staff with a single slide.

1. SITUATION AND CONSIDERATIONS.

a. Area of Interest. Identify and describe those factors of the area of interest that affect functional area considerations.

b. Characteristics of the Area of Operations.

(1) Terrain. State how terrain affects a functional area's capabilities.

(2) Weather. State how weather affects a functional area's capabilities.

(3) Enemy Forces. Describe enemy disposition, composition, strength, and systems in a functional area. Describe enemy capabilities and possible courses of action (COAs) and their effects on a functional area.

(4) Friendly Forces. List current functional area resources in terms of equipment, personnel, and systems. Identify additional resources available for the functional area located at higher, adjacent, or other units. List those capabilities from other military and civilian partners that may be available to provide support in the functional area. Compare requirements to current capabilities and suggest solutions for satisfying discrepancies.

(5) Civilian Considerations. Describe civil considerations that may affect the functional area, including possible support needed by civil authorities from the functional area as well as possible interference from civil aspects.

c. Facts/Assumptions. List all facts and assumptions that affect the functional area.

2. MISSION. Show the restated mission resulting from mission analysis.

3. COURSES OF ACTION.

a. List friendly COAs that were war-gamed.

b. List enemy actions or COAs that were templated that impact the functional area.

c. List the evaluation criteria identified during COA analysis. All staffs use the same criteria.

4. ANALYSIS. Analyze each COA using the evaluation criteria from COA analysis. Review enemy actions that impact the functional area as they relate to COAs. Identify issues, risks, and deficiencies these enemy actions may create with respect to the functional area.

5. COMPARISON. Compare COAs. Rank order COAs for each key consideration. Use a decision matrix to aid the comparison process.

6. RECOMMENDATIONS AND CONCLUSIONS.

a. Recommend the most supportable COAs from the perspective of the functional area.

b. Prioritize and list issues, deficiencies, and risks and make recommendations on how to mitigate them.

Figure 4-2. Generic IO running estimate format

4-21. Running estimate development is continuous. The IO officer maintains and updates the running estimate as pertinent information is received. While at home station, the IO officer maintains a running estimate on friendly capabilities. The unit prepares its running estimate based on researching and analyzing the information environment within its region and anticipated mission sets.

Forces or systems available
- 413 civil affairs BNs
- 344 tactical MISO COs
- 1-55th Signal CO (-) 3x
- 2x EC-130J Commando Solo @ CFACC
- OCO available

Information environment
- Radio is the best medium to reach the civilian population within AO SWORD, followed by social media
- Religious leaders within contested areas are key communicators to the population
- Displaced civilians in camps along main routes may impede coalition forces' advance

Facts
- Civilian and government-controlled media outlets (radio and television) reach population within AO SWORD
- Adversary forces have used civilian radio stations to broadcast coalition forces' troop movements and propaganda in the AO

Assumptions
- Civilian population will support HNSF and coalition forces once security is restored
- Civilian population will remain in place during attack unless there is a loss of essential services

Specified tasks

Identify key communicators within AO SWORD in order to deliver non-interference

Implied tasks
- Deny adversary use of social media messaging during decisive operations
- Develop Soldier and leader engagement, and MISO products to support non-interference

Limitations

MISO messaging and OCO release authority held by CCDR

HPT nominations
- Denial of adversary social media site during decisive operations
- Identify tribal leaders

CCIR nominations
- Block axis of advance by civilian population during attack
- Damage to HN essential services infrastructure and religious structures

EEFI nominations

N/A

Critical planning factors

Air tasking order cycle request 72 hours prior

Objectives

1. Influence civilian population to minimize interference with coalition forces information operations team to prevent civilian casualties

2. Disrupt enemy forces use of media outlets in order to support freedom of movement of coalition forces.

Request for forces

Request OCO to deny use of social media site during decisive operations

AO	area of operations	EEFI	essential element of friendly information
BN	Battalion	HN	host nation
CCDR	combatant commander	HNSF	host-nation security forces
CCIR	commander's critical information requirement	HPT	high-payoff target
CFACC	combined force air component commander	MISO	military information support operations
CO	Company	N/A	not applicable
COMCAM	combat camera	OCO	offensive cyberspace operations

Figure 4-3. Example graphical information operations running estimate

LOGIC OF THE EFFORT

4-22. An essential part of planning and assessing IO is the need to develop an explicit logic of the effort for each objective or effect. The logic of the effort makes explicit how specific efforts lead to attaining objectives. The value of this logic is that its assumptions are made explicit and can become hypotheses that can then be tested and, if necessary, refined. Figure 4-4 provides a simple example of a logic statement and how it evolves when its hypothesis is tested. More complex examples would include additional threat countermeasures that would test each successive hypothesis and refine the IRC mix necessary to create logic that is as foolproof as possible, balanced against risk, available assets, time, and cost.

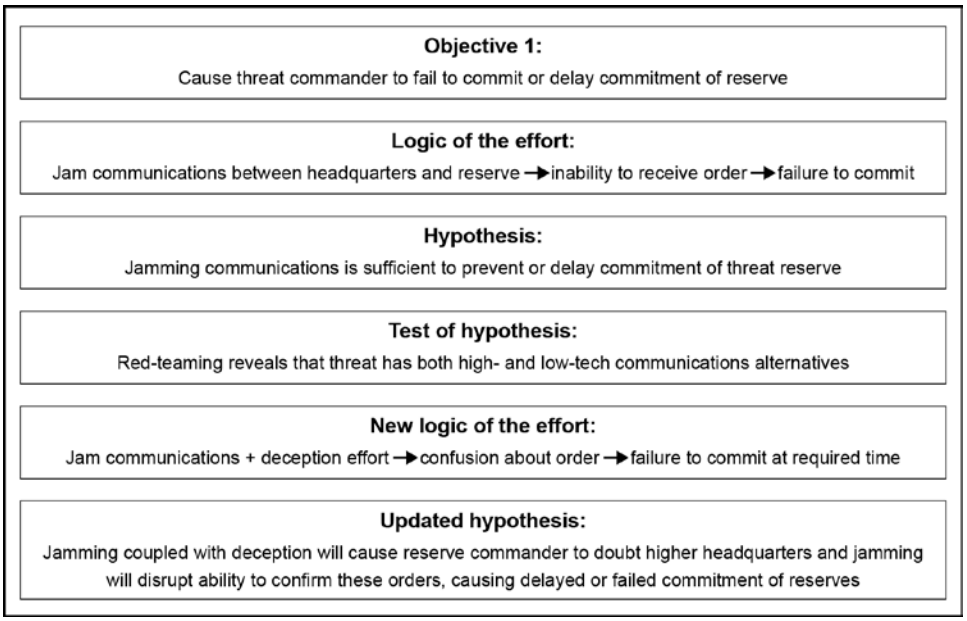

Figure 4-4. Logic of the effort example

COMMANDER'S CRITICAL INFORMATION REQUIREMENTS

4-23. Commander's critical information requirements (CCIRs) identify information needed by the commander to visualize an operational environment and make critical decisions. CCIRs also filter information to the commander by defining what is important to mission accomplishment. If the information operation requires the commander to make a timely tactical decision, then staffs include IO input to the CCIRs, with supporting analysis and input to the decision support template produced during war gaming.

4-24. CCIRs are derived from information requirements, which are maintained and nominated by each staff element to the intelligence or operations staff officer. From the complete array of these requirements, the staff nominates those critical to the commander's decision making to become CCIRs, using the commander's guidance, higher headquarters' CCIRs, the essential-task list, and the IPB (situation template) to narrow and refine the list. Two types of CCIRs exist:

- Priority intelligence requirements.
- Friendly force information requirements.

Priority Intelligence Requirements

4-25. Priority intelligence requirements (PIRs) are information the commander must know about the threat and other aspects of an operational environment. For IO, PIRs focus on conditions in the information environment and adversary actions that affect the information environment. PIRs that may be required for IO include the following questions:

- Hostile forces using or preparing to use a key media outlet to produce or disseminate hostile propaganda.
- Adversary forces preparing to attack friendly information networks (either human or technological).

Friendly Force Information Requirements

4-26. Friendly force information requirements (known as FFIRs) are items of information the commander must know about the friendly force. For IO, friendly force information requirements provide information on

critical aspects of the command's information system, IRCs, and execution of the information operation. Friendly force information requirements that may be required for IO include the following:

- Death or serious injury of noncombatants by friendly forces.
- Media coverage of alleged friendly force misconduct.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

4-27. Essential elements of friendly information (EEFIs) are critical aspects of a friendly operation that, if known by the adversary, subsequently lead to compromise, failure, or limited success of an operation, and, therefore, must be protected from detection. In other words, EEFI is a list of information that must be protected from the adversary's intelligence system to prevent the adversary from making timely decisions and allowing friendly forces to retain the initiative. Typically, EEFI include the command intentions, subordinate element status, or the location of critical assets (such as command posts and signal nodes). EEFI should be refined throughout the planning process, as some information may not be identified until COA development. Once EEFI are developed, measures (as tasks to subordinate units) are developed to protect the information (OPSEC process). Two examples of EEFI are:

- Friendly forces' time of departure for an operation.
- Tribal leaders assisting friendly forces.

INFORMATION OPERATIONS INPUT TO OPERATION ORDERS AND PLANS

4-28. Operation orders and plans are products or outputs of planning. They provide a directive for future action. Commanders issue plans and orders to subordinates to communicate their understanding of the situation and their visualization of an operation. Plans and orders direct, coordinate, and synchronize subordinate actions and inform those outside the unit how to cooperate and provide support (see FM 6-0 for a detailed discussion of operation orders and operation plans). As with all other functions and capabilities, IO provides input to these plans and orders.

Base Orders and Plans

4-29. While every part of an operation order or plan matters, most personnel read the base order or plan (the initial part of the document before the annexes and appendices) because it contains the most mission-essential information. Usually staff sections or specialists involved with a respective function or capability read only those annexes and appendices. If the base order or plan does not contain that information, it might not get read. Increasingly, some aspect of IO is essential to overall operational success. Sections of the base order or plan in which IO may be found include the following:

- Commander's intent, paragraph 3a.
- Concept of operations, paragraph 3b.
- Scheme of IO, paragraph 3c.*x* (*x* is non-specific; the exact subparagraph will vary by order or plan).
- Tasks to subordinate units, paragraph 3j.
- Coordinating instructions, paragraph 3k.

The information contained in these paragraphs and subparagraphs depends on the mission and results of the operations process (an expanded discussion of IO in the operations process appears in FM 3-13 and FM 6-0).

Appendix 15 (Information Operations) to Annex C (Operations)

4-30. The most detailed discussion of IO support to an operation is found in Appendix 15 to Annex C of the operation order or plan. Appendix 15 typically includes several tabs or exhibits that provide the following products or guidance:

- Combined information overlay.
- Synchronization matrix.
- Instructions for IRCs not covered by other appendices, such as operations security, visual information, and combat camera.

4-31. IO officer crafts an IO mission statement while preparing or updating the running estimate. They later refine the mission statement to complete Appendix 15 (IO), which occurs with receipt of an order and commencement of mission analysis. FM 6-0 provides a template for attachments, such as annexes and appendixes. For the mission paragraph (paragraph 2), it instructs planners to state the mission of the functional area to support the base plan or order. In the case of Appendix 15, the functional area is IO.

4-32. The IO mission statement is a short paragraph or sentence describing what the commander wants IO to accomplish and the purpose for accomplishing it. The IO officer develops the proposed IO mission statement at the end of mission analysis based on the unit's proposed mission statement and IO-related essential tasks. During the mission analysis briefing or shortly thereafter, commanders approve the unit's mission statement and CCIRs. They then develop and issue their commander's intent and planning guidance. The IO officer may refine a final IO mission statement based on relevant input from the commander's intent and planning guidance and get it approved by the operations officer. The final IO mission statement includes IO effects and most significant IO-related target categories identified in the information environment during mission analysis. A sample mission statement follows:

> No later than 130600JAN19, IO supports 1 Stryker Brigade Combat Team's defense of key terrain in AO RAIDER by disrupting Donovian command and control and influencing the population of Erdabil Province to support the Government of Atropia to engage the enemy from a position of advantage.

4-33. The mission statement differs from the scheme of IO in its level of detail. The mission statement describes IO in the aggregate. The scheme of IO addresses how IRCs contribute to the scheme and, as a result, accomplish the mission.

Note. There is legitimate debate about whether more than one mission statement can or should exist for a given operation. Some commanders may direct that all attachments reiterate the restated mission in the base order. Functional mission statements are not intended as replacements for the base order mission but, instead, to support it. They are doctrinally justified per FM 6-0.

Scheme of Information Operations

4-34. The scheme of IO begins with a clear, concise statement of where, when, and how the commander intends to employ synchronized IRCs to create effects in and through the information environment to support the overall operation and accomplish the mission. Based on the commander's planning guidance, the IO officer develops a separate scheme of IO for each COA the staff develops during COA development. IO schemes of support are expressed both narratively and graphically, in terms of IO objectives and IRC tasks required to achieve these objectives. Figure 4-5 on page 4-10 provides a sample scheme of an IO statement. Figure 4-6 on page 4-10 illustrates a supporting sketch with articulated objectives and IRCs.

1 SBCT coordinates, deconflicts, and synchronizes IRCs in support of Phase III (Defense) in AO RAIDER. CO collects against Donovian frequencies and communications east of PL MAINE. EW conducts jamming of Donovian armor mission command systems in EAs THOMPSON, UZI, and RUGER. CMOC informs IDPs of collection instructions and safe rally points. MISO influences IDPs to not interfere with military movements and counters Donovian propaganda. The goal of all IRCs is to elicit the surrender or desertion of enemy forces, reduce CIVCAS, and prevent massing of enemy armor and indirect fires. PA controls release of operational information in order to bolster OPSEC and facilitates media engagement strategy to highlight operational successes. Maneuver, CAO, and MISO will conduct SLEs to enable 1 SBCT elements freedom of maneuver throughout AO RAIDER. Finally, 1 SBCT will capture operational successes through COMCAM and other visual information capabilities while OPSEC will protect EEFIs.

AO	area of operations	IDP	internally displaced person
CAO	civil affairs operations	IRC	information-related capability
CIVCAS	civilian casualty	MISO	military information support operations
CMOC	civil-military operations center	OPSEC	operations security
CO	cyberspace operations	PA	public affairs
COMCAM	combat camera	PL	phase line
EA	engagement area	SBCT	Stryker brigade combat team
EEFI	essential elements of friendly information	SLE	Soldier and leader engagement
EW	electronic warfare		

Figure 4-5. Sample scheme of information operations statement

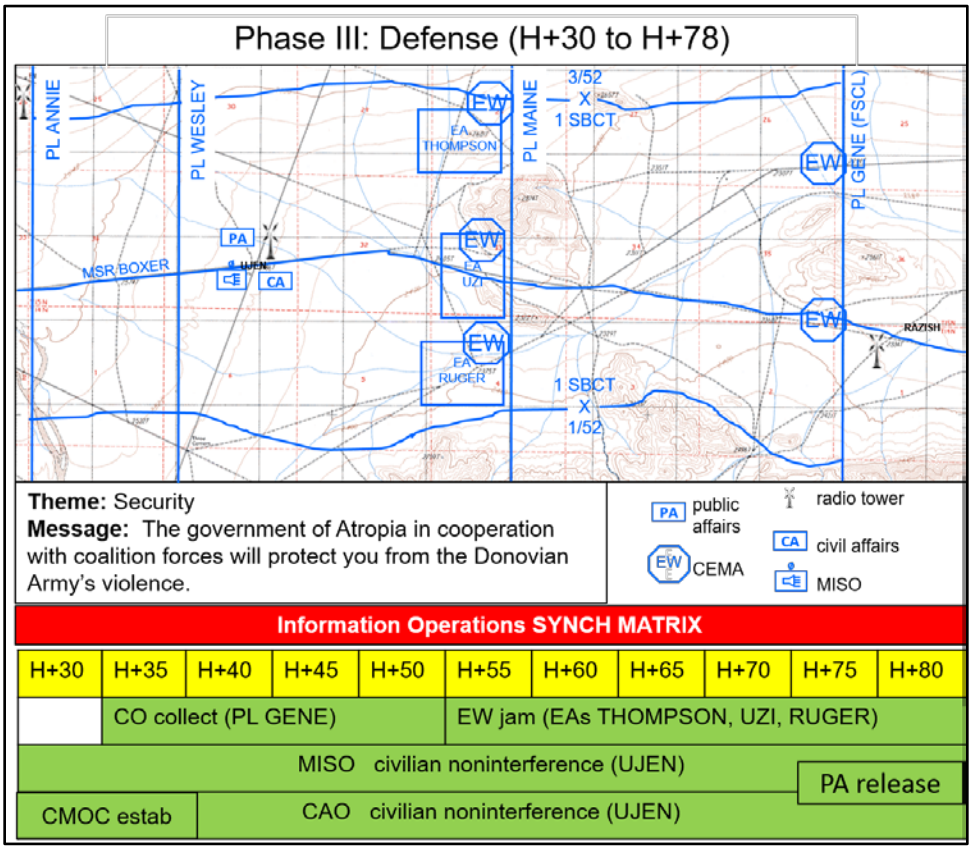

Figure 4-6. Example scheme of information operations sketch

IO Mission Statement: NLT 130600JAN19, IO supports 1 SBCT's defense of key terrain in AO RAIDER by disrupting Donovian C2 and influencing the population of Erdabil Province to support the government of Atropia IOT engage the enemy from a position of advantage.

IO OBJ 1: Influence populace in UJEN to not interfere with 1 SBCT combat operations IOT limit CIVCASs.

IO OBJ 2: Disrupt enemy communications in EAs THOMPSON, RUGER, and UZI to degrade C2 IOT prevent massing of combat power.

Key Tasks

CO/EW

T: Jam Donovian armor mission command systems in EAs THOMPSON, UZI, and RUGER.

P: Degrade C2 capability IOT prevent massing of combat power.

M/MOP: Three precision jamming delivered by tech ops to Donovian C2 systems in EAs THOMPSON, UZI, and RUGER.

MISO

T: Persuade populace in UJEN to not interfere with 1 SBCT movements.

P: Counter Donovian propaganda that misdirects Atropians IOT prevent CIVCASs.

M/MOP: Eight broadcasts by loudspeaker to local nationals vic UJEN.

CAO

T: Inform IDPs of safe rally points.

P: Prevent CIVCASs IOT allow 1 SBCT freedom of movement.

M/MOP: One CMOC established to communicate civil control information with local nationals vic UJEN NLT H+35.

PA

T: Publicize Donovian battle losses to key audiences.

P: Facilitate media engagement strategy IOT highlight operational successes.

M/MOP: Three releases accessible via public sites to key audiences.

MOE 1: Decrease in daily observed number of civilian vehicles or foot traffic on MSR BOXER by 25% from baseline at H+6.

MOE 2: Increase in numbers of tips providing enemy locations and activity by 50% compared to those received at H+6.

AO	area of operations	MISO	military information support operations
C2	command and control	MOE	measure of effectiveness
CAO	civil affairs operations	M/MOP	method/measure of performance
CEMA	cyberspace electromagnetic activities	MSR	main supply route
CIVCAS	civilian casualty	NLT	no later than
CMOC	civil-military operations center	OBJ	objective
CO	cyberspace operations	P	purpose
EA	engagement area	PA	public affairs
estab	establishment	PL	phase line
EW	electronic warfare	SBCT	Stryker brigade combat team
H	hour	synch	synchronization
IDP	internally displaced person	T	task
IO	information operations	tech ops	technical operations
IOT	in order to	vic	vicinity

Figure 4-6. Example scheme of information operations sketch *(continued)*

Information Operations Objectives

4-35. IO objectives express specific and obtainable outcomes or effects that commanders intend to achieve in and through the information environment. In addition to being specific, these objectives enable measurable, achievable, realistic, and time-bounded (known as SMART) measures of effectiveness and performance, which facilitate attaining and assessing established objectives (see Chapter 6 for more details on measures of effectiveness and performance). IO objectives do not stand alone but support the commander's operational intent. Based on the definition of IO, objectives are framed to accomplish the following:

- Attack enemy or adversary decision making and the capabilities or conditions that facilitate that decision making.
- Preserve friendly decision making and the capabilities or conditions that facilitate it.
- Otherwise shape the information environment to provide operational advantage to friendly forces, including freedom of maneuver in this environment.

4-36. For example, if an operational objective is to prevent an enemy force or weapon system from moving from Objective Black before attack, then possible associated IO objectives could be to—

- Disrupt adversary communications within AO Blue to prevent early warning.
- Deceive adversary decision makers on Objective Black to prevent relocation of command and control.
- Influence local populace in Operational Area Blue to support friendly force operations and prevent populace reporting on friendly force activities.

4-37. For each mission or COA considered, IO planners develop IO objectives based on the tasks for IO identified during mission analysis. Depending upon the complexity or duration of the mission (for example, a tactical direct-action mission versus a long-term foreign internal defense mission), there may be only one or numerous IO objectives developed for each phase of the overall operation. Generally, regardless of the mission, no more than five objectives are planned for execution at any one time in the operation.

4-38. Accurate situational understanding is key to establishing IO objectives. Operational- and tactical-level IO objectives must nest with strategic theater objectives. IO objectives further help the staff determine tasks to subordinate units during COA development and analysis.

4-39. No prescriptive format exists for an IO objective. One possible format uses effect, target or target audience, action, and purpose (known as ETAP):

- **E**ffect describes the outcome (for example, influence, destroy, degrade, disrupt, or deceive).
- **T**arget or target audience describes the object of the desired effect.
- **A**ction describes the behavior expected of the recipient.
- **P**urpose describes what will be accomplished for the friendly force.

Chapter 6 provides additional guidance on formulating an IO objective.

Note. Around 2010, the definition of "target" was revised to specify that a target is an entity or object *that performs a function for the adversary*. However, the definition of "target audience" was not similarly adjusted. Per the *DoD Dictionary of Military and Associated Terms*, a target audience is an individual or group selected for influence.

4-40. IO objectives are written in terms of effects, because the desired effect focuses the activities (tasks) of IRCs. For IO, a proper effect falls into one of three categories:

- *Effects against the enemy or an adversary*. IO effects against the enemy or an adversary focus on the threat's ability to collect, protect, and project information. For example, an IO objective might disrupt (effect) an enemy formation's (target) ability to conduct command and control (action) to surprise adversary forces in and around Objective X (purpose).
- *Effects to defend friendly forces*. IO effects regarding friendly forces seek to prevent enemy or adversary interference with friendly abilities to collect, protect, and project information. For example, an IO objective might deny (effect) enemy IRCs (target) the ability to exploit negative effects of friendly force operations (action) to prevent attrition of local populace support away from coalition forces to the enemy (purpose).
- *Effects to shape the information environment*. IO effects shape information content and flow in the operational area's information environment. For example, an IO objective might influence (effect) local populace (target audience) perception of the enemy (action) to increase reporting of enemy activity and locations to coalition forces (purpose).

4-41. Because it is impossible to anticipate all possible effects, terms other than those presented in this publication may be used to describe the desired effects for IO. Effects terms should describe a condition—

not a task. Definitions for the same effect may vary based on the physical, informational, and cognitive nature of the effect and the target of the effect.

4-42. As IO officers develop IO objectives, they establish the criteria—measures of effectiveness (MOEs)—and methods to collect the indicators. If planners cannot identify adequate indications and collection means, then they may need to refine the objective to produce measurable and detectable results. If an objective's MOE is focused on behavior or beliefs, planners must consider physical actions that result from the desired behavior or belief as an indicator.

Information-Related Capability Tasks

4-43. Once IO officers write IO objectives, they develop tasks to subordinate units and staff elements that possess the IRCs needed to accomplish these objectives. These tasks are conveyed through the various types of orders dictated by the MDMP. IRC tasks to subordinate units translate the broad concepts of the objectives into discreet actions. Tasks are often written as—

- **Task**. The task is the action to be performed and the location of the task (for example, prevent local populace interference in Village X).
- **Purpose**. The purpose is the reason why the task is assigned (for example, prevent civilian casualties).
- **Method**. The method describes what unit or capability will conduct the task (for example, MISO Team C121).

4-44. Units take care to ensure that developed tasks do not cause IRCs to violate relevant authorities. For example, MISO tasks are tied directly to Office of the Secretary of Defense-approved MISO objectives (joint) or psychological objectives (Army), which are provided in a MISO program or applicable order. Through direct coordination or the IO working group, IO officers synchronize MISO objectives with IO objectives and align tasks so they support MISO, psychological, and IO objectives simultaneously. Alternatively, if an IO objective requires a MISO task not currently approved, then the IO working group seeks approval through MISO channels, reinforcing the need to plan selected IO objectives well in advance.

4-45. Similar to effects, tasks can be organized into three categories:

- *Tasks against the adversary*. These tasks target threat capabilities and vulnerabilities to collect, protect, and project information (as identified during the COG analysis). An example task might counter enemy propaganda to maintain populace support for capture or kill missions.
- *Tasks to protect friendly forces*. These tasks seek to protect friendly force vulnerabilities in the information environment from threat capabilities to collect and project information. An example task might detect intrusions into friendly force information systems to prevent enemy or adversary collection of critical information.
- *Tasks to shape the information environment*. These tasks shape information content and movement by impacting the key nodes in each subinformation environment to influence local populace perceptions and behavior. An example task might engage religious leaders to bolster friendly credibility and legitimacy.

4-46. Figure 4-7 on page 4-14 depicts how the scheme of IO, IO objectives, and IRC tasks inter-relate to support the MDMP. The relationship among these three is particularly important to the assessment process described in greater detail in Chapter 6.

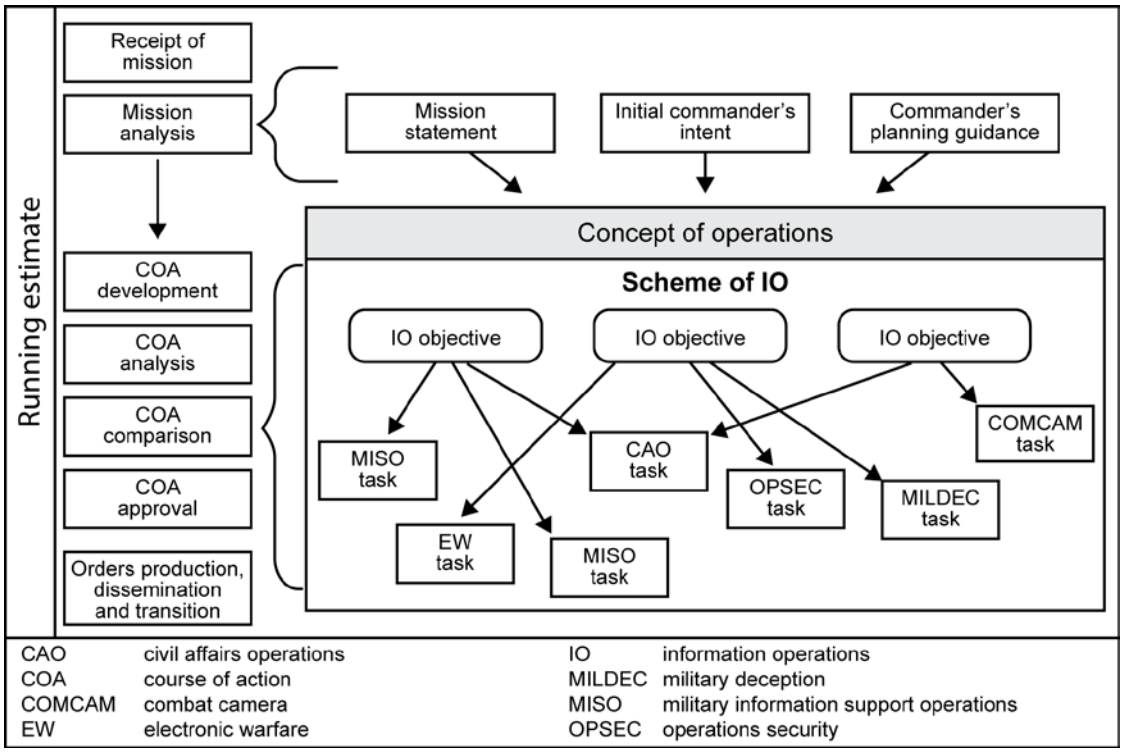

Figure 4-7. Relationship of scheme of IO, IO objectives, and IRC tasks

Information Operations Synchronization Matrix

4-47. The synchronization matrix is used to monitor progress and results of IO objectives and IRC tasks as well as to keep IO execution focused on contributing to the overall operation. It is one of the IO working group's primary tools for monitoring and evaluating progress and assessing whether planned effects have been achieved.

4-48. No specific format exists for a synchronization matrix. The format will be determined by commander's preferences, unit standard operating procedures, mission and situation, and time available. Table 4-1 provides an example matrix that arrays IRC activities by phase. Table 4-2 on page 4-16 provides an alternative example that arrays IRC activities by unit and task.

Table 4-1. Example 1 – Information operations synchronization matrix

IRC	*Phase I*	*Phase II*	*Phase III*	*Phase IV*
EW	Monitor signals of interest. Electronic protection for personnel and equipment.	Electronic attack to disrupt enemy communications. Electronic protection for personnel and equipment.	N/A	N/A
MISO	Broadcast harassment messages against enemy. Broadcast noninterference messages for local populace.	N/A	Broadcast via mobile radio to keep population informed on mission.	Broadcast on mission success. Coordinate with COMCAM for post-mission messaging and countering the effect of adversary information activities.
OPSEC	Determine essential elements of friendly information for mission.	Implement measures to protect essential elements of friendly information to protect movement routes, mission command, and objective.	N/A	N/A
MILDEC	N/A	N/A	N/A	N/A
CAO	Prepare Commander's Emergency Response Program paperwork for funds disbursement. Coordinate with Provincial reconstruction team.	N/A	N/A	Assist personnel returning to villages. Assess small-scale immediate projects.
PA	Prepare press releases. Embed media.	N/A	N/A	Distribute press releases. Conduct press conference and set up interviews with subject matter experts.
COMCAM	Document operation.	Document operation.	Document operation.	Document operation.

CAO	civil affairs operations	MISO	military information support operations
COMCAM	combat camera	N/A	not applicable
EW	electronic warfare	OPSEC	operations security
IRC	information-related capability	PA	public affairs
MILDEC	military deception		

Table 4-2. Example 2 – Information operations synchronization matrix

Tasked unit or system	*IO task*	*Time on target or time of effect*	*Location*	*Remarks*
EA-6B	EW-01	H-1 through H-hour	TAI 002 and 003	Successful if enemy is unable to send early warning
Tactical PSYOP team	MISO-01	H-24 and continue	Objective SPRUCE	Successful if no civilian interference
Civil affairs team	CAO-01	H-24 through H-hour	Objective PINE	N/A
Special Instructions: None				

CAO	civil affairs operations	N/A	not applicable
EA-6B	electronic warfare aircraft (Prowler)	PSYOP	psychological operations
IO	information operations	TAI	target area of interest
MISO	military information support operations		

BATTLE DRILLS

4-49. Battle drills are planning aids designed to speed response to crisis situations occurring during the conduct of a mission. For IO, quick responses to enemy or adversary activities, actions, and events in the operational area are necessary to prevent the enemy or adversary from gaining advantage in the information environment or, conversely, to sustain friendly advantage.

4-50. Staffs develop battle drills during the planning process; however, drills are not complete and final COAs. Rather, battle drills are predeveloped concepts that anticipate crises. Once a crisis occurs, units can adjust the battle drill quickly to address the realities of the situation at hand.

4-51. A military operation can be thought of as a series of events, planned and unplanned, that force both friendly and enemy forces to react to a changing situation. Some of these events, referred to as critical events, directly link to or precipitate mission success of friendly or enemy forces. Critical events—

- Can create both intended and unintended effects and may be brought on by friendly, adversary, or third-party actions.
- Can be either negative or positive. The staff can develop drills that react to either type:
  - For negative critical events, a battle drill should mitigate the impact of the event on the populace and friendly forces.
  - For positive critical events, a battle drill should exploit the event to maximize the impact on the populace and adversary forces.
- Can be triggers or cues for the staff to initiate a battle drill.

4-52. An IO battle drill is a generic scheme of IO that addresses a friendly force IO response to a critical event that may occur during execution of the operation. While no doctrinally established format exists for a battle drill, its format should mirror existing products or follow unit standard operating procedure. Battle drills are developed to suit specific missions and potential branches and sequels of missions. Each battle drill should—

- Identify critical events.
- Define the desired information end state.
- Develop the scheme of IO.

The information contained in a battle drill is not a final and complete plan but rather a concept that must be refined to the realities of the situation at hand.

Identify Critical Events

4-53. Planners determine what critical events may result from friendly, enemy, adversary, or third-party action. Planners focus on events that will either occur in or affect the information environment and are

significant enough to affect the command's mission. The following list provides some examples of critical events:

- Civilian collateral damage.
- Civilian casualties.
- Fratricide incidents.
- Populace interference with friendly force operations (for example, civil demonstrations).
- Quick reaction force deployment.
- Adversary or friendly forces violation of law of land warfare (for example, atrocities against civilians, mass-grave discovery).
- Environmental incident (for example, hazardous material spill).
- Propaganda directed against friendly forces.
- EEFI or any other sensitive or classified information disclosure.

Define Information End State

4-54. Battle drills are designed to respond to specific situations. These situations must be sufficiently defined so planners can adjust the battle drill's concept to compensate for the differences between the planned and actual situations. For IO, this means defining the information end state for each battle drill. Examples of information end states for mitigation and exploitation battle drills are as follows:

- A mitigation battle drill:
  - *Event*. Disclosure of EEFI or classified information.
  - *Target*. Adversary.
  - *Information end state*. Adversary decision makers cannot take advantage of sensitive information about the friendly force.
- An exploitation battle drill:
  - *Event*. Destruction of key infrastructure by enemy forces.
  - *Audience or recipient*. Populace.
  - *Information end state*. Populace is mobilized to support friendly forces against the enemy to prevent future attacks.

Develop Battle Drill Scheme of Information Operations

4-55. The scheme of IO is a concise and easily understandable word picture describing how IRCs may be employed and what staff coordination must be conducted to employ these capabilities. The scheme must be integrated with the overall operation. How much information is known when the battle drill is created determines its level of detail.

4-56. As part of the scheme of IO, leaders develop tasks, purposes, methods, and means, and, if appropriate, targets for each participating IRC. A purpose for each task is included to explain each IRC's part in the operation. If appropriate, general target sets are identified for each tasked IRC. All IO-relevant capabilities—maneuver units and those staff entities that may have important roles in responding to the battle drill event—are considered. A purpose for each task is included to maximize IRC initiative. IRCs develop measures of performance (MOPs) for their assigned tasks.

4-57. Figure 4-8 on page 4-18 provides a sample format for a battle drill. Leaders modify the format as needed to fit the situation, mission, and commander's preference. Figure 4-9 on page 4-19 illustrates an abbreviated staff battle drill.

SITUATION: Insurgent forces attack friendly forces, a friendly third-party organization, or an opposing faction (for example, a bombing, shooting, or mortar attack).

ASSUMPTIONS: The insurgent attack does not cause significant friendly causalities.

LIKELY FRIENDLY ACTION: A response force is deployed to secure the site and find and destroy the insurgent force. Security operations are conducted in and around the area of attack. If necessary, force protection measures are increased.

SCHEME OF IO: Gain populace support for counterinsurgency activities and identify hidden insurgent cells for targeting. IRCs provide direct support to the response force. MISO teams disseminate print products to the populace near the attack site. Unit leaders, MISO teams, and CAO teams engage local leaders to gain support for friendly operations. PA issues a press release to explain the command's position and counter misinformation concerning the situation.

Restrictions: MISO products must conform to and support approved programs.

Measure of Effectiveness: Increase reporting by populace of insurgent activity by 15% compared to the level of reporting before attack.

Capability	Key Tasks	Purpose	Method	Target or TA
MISO	Disseminate print products and radio broadcasts to the populace of villages in and around the attack site.	Identify hidden insurgent cells. Reduce populace support for insurgent forces and activities.	Handbills and posters. Contract radio.	Local populace. Insurgent fence sitters.
SLE	Engage local leaders.	Gain support for counterinsurgency activities.	Face-to-face.	Civil leaders.
PPP or CMO	Response force decreases threatening signatures or activities without compromising force protection.	Build rapport and gain support for counterinsurgency activities.	Soccer matches.	Local populace

CAO	civil affairs operations	PA	public affairs
CMO	civil-military operations	PPP	presence, profile, and posture
IO	information operations	SLE	Soldier and leader engagement
IRC	information-related capability	TA	target audience
MISO	military information support operations		

Figure 4-8. Sample battle drill format for insurgent-related violence

1. **Situation**: React to collateral damage resulting from coalition-force action.

2. **Information end state**: Preempt adversary propaganda and negative media reporting.

3. **Immediate** (onsite):
- Notify commander.
- Document the scene (for example, COMCAM photos).
- Conduct on-site key-leader engagement to determine facts and conduct initial mitigation.

4. **Within 2 hours**:
- Notify operational area owner.
- Notify local-government officials.
- Public affairs makes a public statement of the facts for broadcast by local print, radio, and TV media.

5. **Within 24 hours**:
- Conduct key-leader engagements with local elders using HN partner-unit commanders, coalition commanders, and local-government officials.
- Assess damage for possible CAO projects.

6. **After 24 hours**:
- Coordinate for follow-up media coverage and key-leader engagement by operational-area owner.
- Compensate families (if appropriate) and conduct CMO or CAO activities.

CAO	civil affairs operations	HN	host nation
CMO	civil-military operations	TV	television
COMCAM	combat camera		

Figure 4-9. Sample abbreviated battle drill format

This page intentionally left blank.

Chapter 5

Coordination of Intelligence Support and Integration of Information Operations into Targeting

INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS

5-1. An important synergy exists between IO and the intelligence and fires warfighting functions. Among the doctrinal tasks of the intelligence warfighting function is providing support to IO, IRCs, and targeting. The integration of IO into the targeting process—a task managed within the fires warfighting function—is important to mission accomplishment across the range of military operations.

5-2. *Intelligence* is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations (JP 2-0). IO planning and execution rely on the existing intelligence capabilities of the command to provide support. IO significantly increases the demand for intelligence to support detailed analysis of the information environment and the adversary's use of the information environment.

5-3. Intelligence support to IO is an intelligence community task. Agencies outside the intelligence community provide information that contributes to the overall support of IO that is integrated into intelligence products supporting the mission. The intelligence staff is responsible for coordinating and overseeing all command intelligence; however, each staff section and element involved in planning and execution has a responsibility to assist in this task. Thus, IO planners work closely with intelligence personnel throughout the intelligence process to ensure ethical, effective, and efficient intelligence support. Additionally, the IO staff conducts its own research and analysis.

5-4. Intelligence support to IO is continuous and typically requires long-lead times. The intelligence necessary to affect the perceptions and decision making of enemies, adversaries, or other audiences often requires that units position and employ specific sources and methods to collect the information and conduct the analyses needed for the information operation. The challenge is to get the right information and intelligence at the right time.

5-5. As in other intelligence activities, intelligence analysts should avoid describing or portraying the adversary's actions in the information environment as a mirror image of friendly IO concepts, doctrine, and tactics, techniques, and procedures. Culturally, the enemy or adversary is unlikely to think or act as the United States does.

5-6. Key terms used in this section are defined below:

- *Information requirement*. Any information elements the commander and staff require to successfully conduct operations (ADRP 6-0).
- *Intelligence requirement*. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces (JP 2-0).
- *Priority intelligence requirement*. An intelligence requirement that the commander and staff need to understand the threat and other aspects of the operational environment (JP 2-01). The commander designates PIRs. Information requirements not designated by the commander as PIRs become intelligence requirements.

- *Intelligence estimate*. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption (JP 2-0).
- *Intelligence preparation of the battlefield*. The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations (ATP 2-01.3).

INFORMATION OPERATIONS AND THE INTELLIGENCE PROCESS

5-7. All intelligence for the commander and staff, including that needed for IO, is produced as part of the intelligence process. By working closely with the intelligence staff officer during the intelligence process, IO planners can minimize intelligence gaps and maximize available intelligence and collection assets to develop a reasonably accurate understanding of the information environment and a representative and reliable model of adversary operations in the information environment. To integrate into the intelligence process, IO planners—

- Identify IO-specific intelligence gaps concerning the information environment and adversary operations in the information environment, recommend intelligence requirements as PIRs, and submit requests for information to fill the gaps.
- Become familiar with available collection assets, capabilities, and support relationships (direct support or general support). Planners determine time requirements for each collection asset and consider the capabilities and limitations of the assets that will perform the mission.
- Coordinate with the collection manager to ensure information requirements for IO are considered for inclusion as collection tasks. Ensure that IO-specific information requirements are matched to the correct information collection asset.
- Establish relationships with key intelligence personnel.
- Vet all intelligence products developed from reachback support and other external sources through the intelligence staff officer to avoid disconnected analysis.
- Provide feedback on the quality of intelligence provided and its usefulness to facilitate refinement.
- Assess the intelligence support provided to improve the working relationship with the intelligence staff while providing feedback to the intelligence analyst for improvements.

INTELLIGENCE "PUSH" AND "PULL"

5-8. Intelligence is disseminated by the "push" or "pull" principle. For "push," IO planners coordinate with the intelligence staff to get access to the dissemination means that have IO-pertinent products. This is accomplished by working with the intelligence analysts to get IO-specific information requirements injected into the collection cycle, nominating PIRs for either the information environment or adversary actions in the information environment, and coordinating with higher headquarters' IO staffs to routinely receive distribution of intelligence products. To "pull" intelligence from the intelligence staff, IO planners coordinate for access to those assets and systems that have IO-relevant information and intelligence, attend intelligence staff updates and fusion meetings, and coordinate with units.

5-9. Publically available information is an often overlooked way to get information and intelligence. Much useful information about the populace and media is available from public sources, including social media. This information often addresses the IO's information requirements. Like other aspects of planning, IO planners conduct their own open-source research.

REQUESTS FOR INFORMATION

5-10. Intelligence production is requirements-driven. Units use requests for information to request specific information and intelligence. Each command has its own requests for information format and procedures; however, each observes the following rules when developing requests for information:

- **Conduct initial research**. Units try to find the information or intelligence on their own, using requests for information to get information not readily available. Units list sources already checked so the intelligence analyst does not waste time working with materials and products that lack the requested information.
- **Clearly state the requirement**. Units describe—as specifically as possible—the information needed. Units avoid language and terms associated solely with IO, as well as requests for a particular type of intelligence (for example, signals or human intelligence). Units limit requests for information to one question per request.
- **Justify the request**. Units articulate why the request is important. For greater priority, units tie the requests for information to a PIR.
- **State accurately the latest time the information will be of value**. Units state when information will no longer be useful, being truthful about the date. The information that units provide affects collection management and assets dedicated for higher-priority missions.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

5-11. The basis of intelligence support to IO is the IPB process, a prerequisite to planning any operation. The intelligence staff officer, with assistance and input from the staff, uses IPB to define the AO, describe the area of interest, describe the IPB's effects, evaluate the threat, and determine threat courses of action. During IPB, the IO officer works with the intelligence staff section to determine threat capabilities and vulnerabilities in the information environment regarding both the threat and other relevant targets and audiences in the AO and to determine IO-related factors to consider during each IPB step (see discussion beginning with paragraph 2-8 for analyzing the information environment and adversary operations in the information environment).

INFORMATION OPERATIONS INTEGRATION INTO TARGETING

5-12. Even before planners integrate IO into targeting, they integrate it into Army design methodology and planning; it cannot be an afterthought. Although IO synchronizes IRCs to create both lethal and nonlethal effects, commanders often consider nonlethal IO effects as secondary to lethal effects, particularly at lower echelons. As a result, commanders have tended to request them late or after-the-fact. Given the long lead times that several IRCs require to secure authorization or create effects, this last-minute approach to their employment prevents their effects from being either timely or effective.

5-13. Army design methodology, planning, and targeting are the overarching processes used to support decision making and mission accomplishment. They form the basis for identifying and then integrating lethal and nonlethal actions necessary to achieve the commander's intent. Army design methodology focuses on comprehending the problem, understanding the operational and information environments, and developing an operational approach that underpins subsequent planning. Planning focuses on solving the problem by developing detailed plans and concepts of operation. Targeting enables units to select and prioritize targets and then match the appropriate lethal and nonlethal responses to them. Commander's intent and guidance, as developed in design and planning, largely drive targeting. The commander provides guidance on objectives, priorities, and lethal and nonlethal effects (for example, deny, disrupt, delay, suppress, neutralize, destroy, or influence).

TARGETING OVERVIEW

5-14. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). A *target* is an entity or object that performs a function for the adversary considered for possible engagement or other action (JP 3-60). It may be an area, complex, installation, force, equipment, capability, function, individual, group, system, entity, or behavior identified for possible action to support the commander's intent, objectives, and guidance. Targets relate to objectives at all levels—strategic, operational, and tactical. *Fires* is the use of weapon systems or other actions to create specific lethal or nonlethal effects on a target (JP 3-0). The nature of the target or threat, the conditions of the mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations), and desired outcomes determine whether actions need to be lethal or nonlethal.

TARGETING PROCESS CONSIDERATIONS

5-15. FM 3-13 provides an overview of IO and targeting and ATP 3-60 is the Army's targeting primer. Paragraphs 5-16 through 5-23 discuss additional considerations for commanders and staffs on integrating IO into the targeting process or methodology.

Note. In this discussion, targeting process, cycle, and methodology are used synonymously.

Various Targeting Cycles

5-16. While targeting occurs at all echelons, it expands dramatically at the operational and strategic levels. Tactical maneuver units will almost exclusively employ the *decide, detect, deliver, and assess* (known as D3A) targeting process. Brigade and above elements employ a mix of cycles, depending on whether they are executing a multi-domain battle or participating in joint operations or both (see figure 5-1). Actions that can create effects on targets are identified in the IO working group. These actions against specific targets are submitted to the targeting working group and ultimately the targeting board for approval.

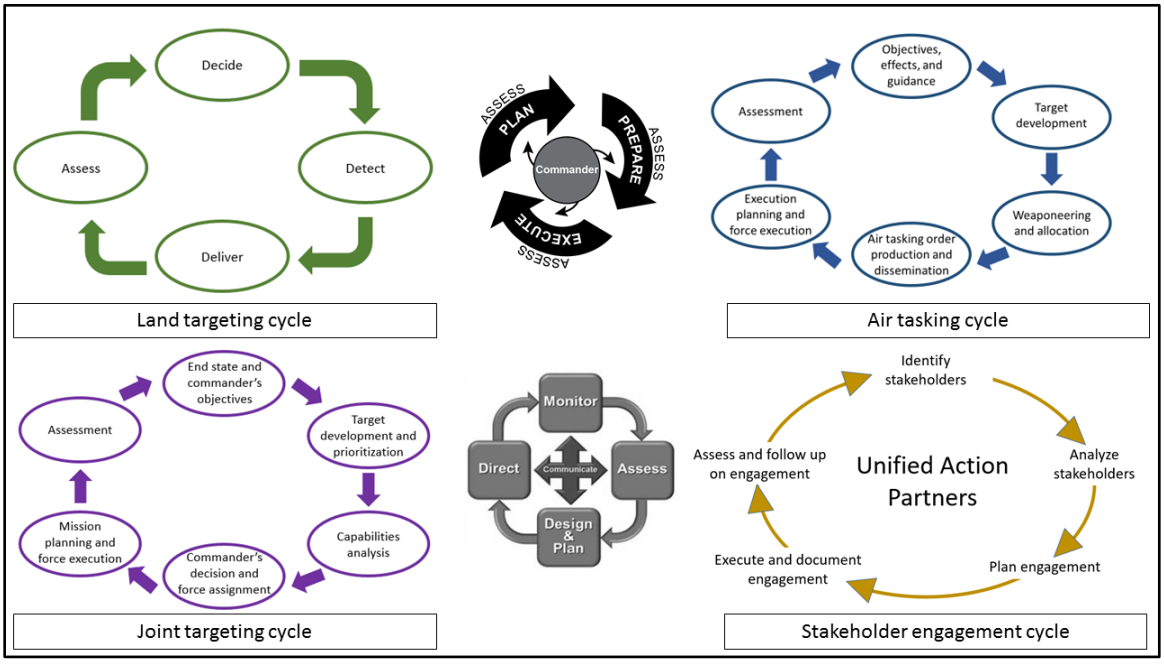

Figure 5-1. Various targeting processes that contribute to decision making and mission accomplishment

Targeting Categories

5-17. Two categories of targeting exist: deliberate and dynamic. Deliberate targeting includes planned targets either scheduled or on-call. Dynamic targeting includes targets of opportunity identified too late or not selected in time to be included in deliberate targeting. Targets of opportunity can be unplanned or unanticipated.

5-18. Soldier and leader engagements (SLEs) provide an example of each category. Deliberate SLEs, such as key leader engagements, are planned and rehearsed before execution, and can either be scheduled or on-call. Deliberate SLEs have a specific actor or subject identified as part of the planning process and are tailored to that specific person. Dynamic SLEs are impromptu. While often unanticipated, they can still benefit from prior planning that focuses less on the subject (actor) of the engagement and more on the process.

5-19. Given the long-lead times associated with employing certain IRCs, greater time may be needed to enable the appropriate response. MISO and IJSTO are two IRCs, in particular, that may have lengthy approval processes. To support dynamic targeting, PSYOP forces arrange an abbreviated approval process; rely on produced, approved, and pre-positioned products, when possible; and plan early based on target lists, identifying targets that will likely be dynamic. See Table 5-1 for targeting tasks.

Table 5-1. Information operations-related targeting tasks in relation to the decide, detect, deliver, and assess targeting process functions

	Operations process activity	***Targeting process function***	***Targeting task***
Assessment	**Planning**	**Decide**	**Mission Analysis** • Develop IO-related HVTs • Provide IO input to targeting guidance and targeting objectives **COA Development** • Designate potential IO-related HPTs • Contribute to the threat and vulnerability assessment • Deconflict and coordinate potential HPTs **COA Analysis** • Develop HVT list • Establish target selection standards • Develop AGM • Determine criteria of— ▪ Successful battle damage assessment ▪ Requirements **Orders Production** • Finalize HPT list • Finalize target selection standards • Finalize AGM • Submit IO information requirements or requests for information to intelligence staff section
	Preparation **Execution**	**Detect**	• Execute collection plan • Update PIRs or IO information requirements as they are answered • Update HPT list and AGM
		Deliver	• Execute attacks in accordance with the AGM
		Assess	• Evaluate effects of attacks • Monitor targets attacked with nonlethal IO

AGM	attack guidance matrix	HVT	high-value target
COA	course of action	IO	information operations
HPT	high-payoff target	PIR	priority intelligence requirement

Deliberate Targeting

5-20. Table 5-1 depicts the interrelationship among the operations process, the deliberate targeting process, and the IO-related targeting tasks that must be accomplished to ensure IO efforts are planned and executed to support the overall mission. In the sections that follow, emphasis lies on the following IO-related tasks:

- IO input to the high-payoff target list.
- IO input to target selection standards.
- IO input to the attack guidance matrix.

5-21. High-payoff targets (HPTs) are managed in the high-payoff target list. HPTs are a subset of high-value targets—targets the enemy requires for successful completion of its mission. An HPT is a target whose loss to the enemy will significantly contribute to friendly mission success. Table 5-2 provides examples of HPTs that the IO working group would submit to the targeting working group as nominations.

Table 5-2. Sample information operations input to high-payoff target list

Phase 1 – Isolate the enemy unit		
Priority	***Category***	***High-Payoff Targets***
1	Fire Support	Data link between target acquisition radars and fire direction center
2	Command and Control	Enemy leader's social media sites
3	Maneuver	Militia company-level leaders

5-22. Target selection standards address accuracy or other specific criteria that units must meet before they can engage targets. Standards usually consist of several elements—including HPTs, timeliness, and accuracy—although units can develop their own target selection standards worksheets. The HPT refers to the designated HPT that the collection manager is tasked to acquire. Timeliness refers to the time window within which units report valid targets to weapon systems. Accuracy concerns the allowable target location error for the target. The criteria are the least restrictive target location error given the capabilities of available weapon systems. Table 5-3 provides examples of IO-related target selection standards.

Table 5-3. Sample information operations input to target selection standards

Target Selection Standards Worksheet		
High-payoff target	***Timeliness***	***Accuracy***
Observation posts	60 minutes	500 meters
Broadcast tower	480 minutes	100 meters

5-23. The attack guidance matrix (AGM) provides guidance on what HPTs units should engage and when and how units should engage them (see table 5-4). Although units may develop their own AGM format, the matrix typically includes the following elements:

- *High-payoff target*. The high-payoff target column is a prioritized list of HPTs by phase of the operation.
- *When*. This column indicates the time the target should be engaged.
- *How*. This column indicates the weapon system that will engage the target.
- *Effect*. The desired effects on the target or target system are stated in this column.
- *Remarks*. Remarks concerning whether or not assessment is required, whether coordination must occur, and any restrictions are indicated in this column.

Table 5-4. Sample information operations input to attack guidance matrix

High-payoff target	***When***	***How***	***Effect***	***Remarks***
Ops	I	Field artillery	Destroy	Use search and attack teams in restricted areas
Militia	I	CO	Neutralize	Destroy command and control
Cell phone	A	EA	Disrupt	Disrupt service starting H-2
Violent IDP crowds	A	MISO or MP	Disperse	25 or more constitute MSR blockage

A	as acquired	IDP	internally displaced person
CO	cyberspace operations	MISO	military information support operations
EA	electronic attack	MP	military police
H-2	hour minus two (representing 2 hours before)	MSR	main supply route
I	immediate	OP	observation post

Dynamic Targeting

5-24. Dynamic targeting uses the find, fix, track, target, engage, and assess (known as F2T2EA) process (figure 5-2). Table 5-5 summarizes the IO-related inputs or activities that support each phase of the process.

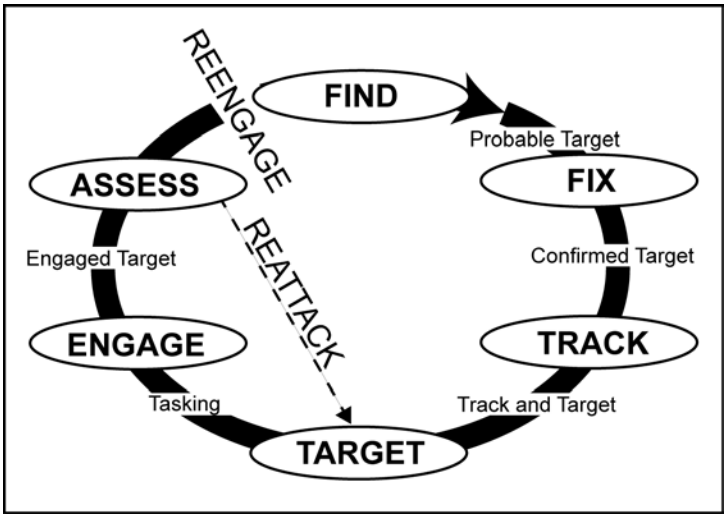

Figure 5-2. Dynamic targeting

Table 5-5. Information operations inputs and activities to support find, fix, track, target, engage, and assess

Function	*IO Input or Activity*
Find	• Updated and focused CIO. • IO input to collection plan. • IRCs reporting of potential targeting signatures.
Fix	• IO updates to targeting. • IRCs tasked to report information during mission performance to develop target. • Targets' information-related vulnerabilities.
Track	• Requests for information for target location refinements. • Targets' information-related vulnerabilities updated. • IO input to risk assessment and collateral damage estimate (2nd and 3rd order effects). • IRCs deconflicted.
Target	• IRC tasks developed to achieve desired effect. • MOEs and MOPs also developed.
Engage	• Approved IO tasks in mission order. • IRCs employed to conduct, support, and reinforce engagement. • Initial reports of results from subordinate units as means to monitor MOPs.
Assess	• MOEs assessed against baseline. • CIO updated. • Re-engagement recommendations submitted.

CIO	combined information overlay	MOE	measure of effectiveness
IO	information operations	MOP	measure of performance
IRC	information-related capability		

INFORMATION OPERATIONS TARGET NOMINATIONS AND THE TARGETING SYNCHRONIZATION MATRIX

5-25. As revealed in figure 4-1 on page 4-4, an important output of the IO working group that feeds into the targeting working group is target nominations. The format for these nominations is a targeting synchronization matrix such as the one shown in figure 5-3.

	PHASE III											
	DECIDE					DETECT	DELIVER			ASSESS		
HPT/ PRI	TGT set	TGT #	TGT description	Desired effect	Phase	Asset	Asset	How	When	Asset	Measure of effectiveness	Status
1	- Arianan forces	IRC032	Arianan resolve; surrender messaging (OBJ COLORADO)	Degrade	IIIB	HUMINT, IMINT, and SIGINT	1/1, 2/1, 3/1 CAV & 110 MEB (loudspeaker and handbills)	Planned	D+9 - D+10	1 ID	15% of Arianan forces desert or surrender to coalition forces	DL - DM
1	Arianan forces	IRC033	Arianan forces (upon retrograde)	Influence	IIIB	HUMINT, IMINT, and SIGINT	Press release or radio and TV broadcast; COMCAM	Planned	D+9 - D+10	CJTF; 1 ID	75% of local media reports Arianan forces retrogade and treatment of EPWs; 5% increase in surrenders and desertions	DL - DM
2	Atropian 348th BDE, commission on refugees or IDPs & RCC directors	IRC034	Assess IDPs mitigation (OBJ OVERLORD)	Assess	IIIB	HUMINT	110 MEB SLE	Planned	D+10	1 ID	75% of acute essential service needs identified and development or coordination of responses	DM
2	Ministry of Internal Affairs & USAID	IRC035	Assess IDPs mitigation (OBJ CEDAR FALLS)	Inform	IIIB	OSINT and HUMINT	300 SB SLE	Planned	D+10	1 ID	1 ID informed on PH IV engagement requirements; 75% coordination between IA, 1 ID, and host nation	DM
1	Local security forces	IRC036	Coordinate and synchronize for PH IV operations (OBJ CEDAR FALLS)	Coordinate	IIIC	OSINT and HUMINT	Victory 6 SLE	Planned	D+11	CMOC, G-9	75% of local security forces engaged and leading local security efforts with minimal coalition support	DN

Figure 5-3. Example targeting synchronization matrix reflecting IO target nominations

Chapter 6
Assessment

ASSESSMENT PURPOSE

6-1. The purpose of assessment is to support the commander's decision making. Commanders continuously assess the situation to better understand current conditions and determine how the operation is progressing. Continuous assessment helps commanders anticipate and adapt the force to changing circumstances. Commanders incorporate assessments by the staff, subordinate commanders, and unified action partners into their personal assessments of the situation. Based on their own assessments, commanders modify plans and orders to adapt the force to changing circumstances. Assessment is a staff-wide effort, not simply the product of a working group or a particular staff section or command post cell. Assessment of IO objectives and effects is an integral part of the staff-wide assessment process. Assessment requires a commitment of resources that must be balanced against other competing requirements and priorities of work; however, without sufficient resources, assessments often prove ineffective or fail altogether. This means that the IO officer will need to negotiate and prioritize this effort to make it meaningful to support decision making.

ASSESSMENT FRAMEWORK

6-2. All plans and orders have a general logic. This logic links tasks given to subordinate units with achieving objectives and achieving objectives with attaining the operation's end state. An assessment framework incorporates the logic of the plan and uses measures—MOEs and MOPs—as tools to determine progress toward attaining desired end state conditions, as shown on figure 6-1 (see discussion beginning in paragraph 6-17 for more information about MOEs, MOPs, and indicators).

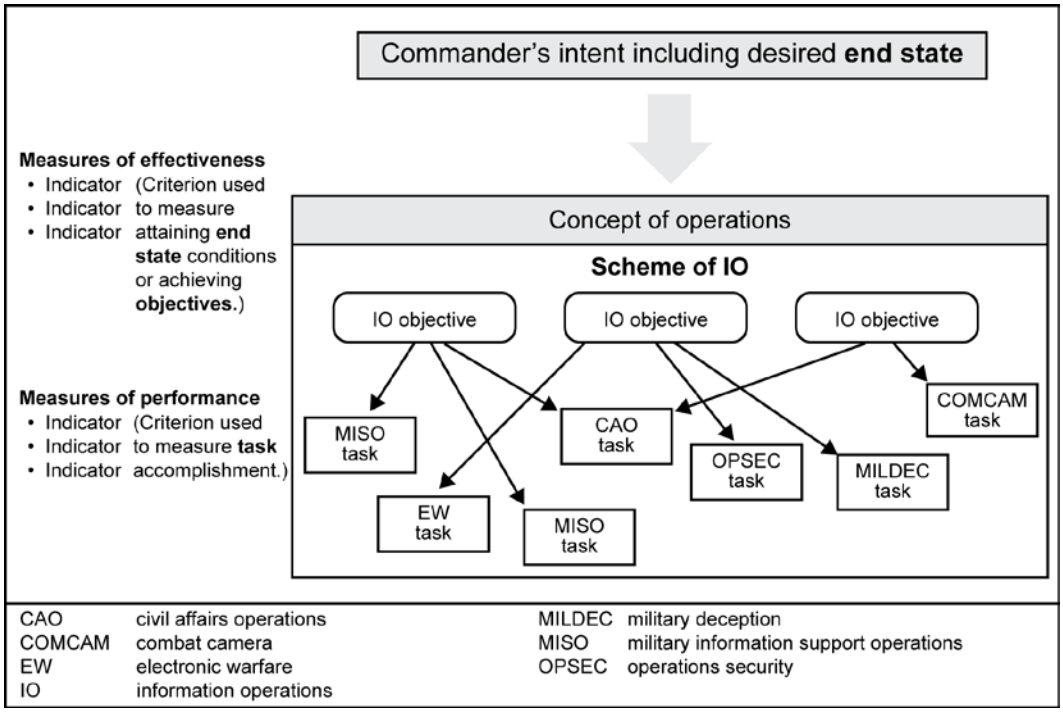

Figure 6-1. Framework for assessment

ASSESSMENT FOCUS

6-3. Different levels of headquarters likely have different assessment focuses. Tactical-level units focus primarily on task assessment. Operational-level units focus on environmental (operational and information) assessment. Strategic-level units focus on campaign assessment. Table 6-1 summarizes the various aspects that differentiate one level of focus from another.

Table 6-1. Aspects of assessment by level of focus

Assessment Focus			
Assessment aspect	***Task***	***Environment***	***Campaign***
Source (basis) for criteria	Directed tasks in OPORD or OPLAN.	Desired conditions in OPLAN or OPORD.	End state objectives (success criteria).
Criteria	Primarily MOP.	Primarily MOE.	MOE.
Time horizon	Near (daily).	Mid (weekly or monthly).	Long (monthly, quarterly, or annually).
Indicators	Largely quantitative; may have qualitative commander input.	Mixed-method.	Mixed-method.
Collection means	Reports, SIGACTs, subordinate commanders, circulation.	Reports, polls, media analysis, subordinate commanders, stakeholders, circulation.	Reports, polls, media analysis, subordinate commanders, stakeholders, circulation.
Analysis and evaluation	Current operations centric, after action review, and commander qualitative.	Staff analysis and evaluation through staff-wide efforts, with focused ad hoc assessment cell or working group. Commander parallel evaluation based on qualitative (opinion-based) indicators through commander crosstalk and circulation. Informed by staff efforts.	Combination of the quantitative staff efforts and commander qualitative analysis and evaluation. Trend analysis.
Commander – Staff interface venues	Daily updates, after action review.	Periodic OE or information environment staff assessment updates; commander's circulation reports.	Formal assessment briefings and conferences.
Actions for improvement	Task refinement, changes to quantities or methods of delivery, additional IRC support, and reengagement or repetition of IRC tasks.	Better understanding of local culture, improved information environment analysis, message refinement, and reengagement by alternate means.	Reassessment of campaign strategy, refinement of commander's end state, and expansion of IO planning and execution, including unified action partners.

IO	information operations	OE	operational environment
IRC	information-related capability	OPLAN	operation plan
MOE	measure of effectiveness	OPORD	operation order
MOP	measure of performance	SIGACT	significant activity

TASK ASSESSMENT

6-4. A task assessment asks whether units or IRCs are performing assigned or implied tasks to standard using MOPs. Task assessment answers the question, "Are we doing things right?" as well as follow-on questions such as, "Was the task completed?" and "Was it completed to standard?"

INFORMATION (AND OPERATIONAL) ENVIRONMENT ASSESSMENT

6-5. Environment assessment asks whether units are achieving the necessary objectives and conditions—MOEs-oriented—in the information and operational environments necessary to accomplish the mission. This type of assessment answers the question, "Are we doing the right things?"

CAMPAIGN ASSESSMENT

6-6. Campaign assessment is undertaken at the theater level (such as the geographic combatant command) in the area of responsibility to assess whether units achieve theater strategic or campaign objectives (objective-oriented). This type of assessment answers questions about progress toward accomplishing the mission. Campaign assessment also includes long-term strategic assessments focused on theater engagement objectives and the ethical, effective, and efficient application of resources.

ASSESSMENT METHODS

6-7. Assessments can be quantitative or qualitative or both (mixed method). One method is not necessarily better than another. The various components of the assessment framework—end state, objectives, and tasks, as well as the type of intelligence or information gathered—all govern which method is best suited to yield the feedback necessary to support decision making and operational adjustments.

QUANTITATIVE

6-8. Objectives that are specific, measurable, achievable, realistic, and time-bounded (known as SMART) lend themselves to quantitative assessment because they employ MOEs that are similarly specific and measurable. A quantitative methodology is well-suited for almost all task-level assessments and selected environment and campaign assessments. By its nature, quantitative methodology is data-centric and requires the requisite automated systems and personnel expertise to employ it effectively. Quantitative assessment tends to be staff-centric and is often a check on commanders' more subjective, qualitative assessment.

QUALITATIVE

6-9. Effective qualitative assessments require the same rigor, if not more, as quantitative assessments and benefit from expertise in their design and conduct. The IO officer, IRCs, functional staff leads, and members of a working group or ad hoc assessment cell assist with the design and conduct of qualitative assessments (just as they do with quantitative assessments). For MOPs, the IRCs are the best resource for whether an activity has started, or is completed, and the standards to which it was performed. For MOEs, the IO officer—working with the intelligence staff and other members of the staff—assesses for the commander whether, and to what extent, units achieve effects in the information environment. To the degree possible, qualitative assessments are enhanced by turning qualitative information into quantitative values. This process helps remove subjectively and facilitates the compilation and reporting of findings.

MIXED-METHOD

6-10. Mixed-method or blended assessments combine quantitative and qualitative assessment methodologies to gain the best of both. IO, in particular, benefits from mixed-method assessments due to the diverse range of effects it can create in the information environment, from directly observable physical effects to long-term cognitive effects.

ASSESSMENT PROCESS

6-11. Assessment involves three inter-related phases: monitoring, evaluation, and adjustment (directing action for improvement). FM 6-0 discusses each of these phases in detail. In the evaluation phase, three sets of criteria are employed to evaluate progress: MOEs, MOPs, and indicators.

MONITORING INFORMATION OPERATIONS

6-12. *Monitoring* is continuous observation of those conditions relevant to the current operation (ADRP 5-0). Monitoring within the assessment process allows staffs to collect relevant information, specifically that information about the current situation that staffs can compare to the forecasted situation described in the commander's intent and concept of operations. Progress cannot be judged, nor effective decisions made, without an accurate understanding of the current situation.

6-13. The IO officer monitors IRCs to determine progress towards achieving the IO objectives. Once execution begins, the IO officer monitors the threat and friendly situations to track IRC task accomplishment, determine the effects of IO during each phase of the operation, and detect and track any unintended consequences. The IO officer works closely with the intelligence cell, intelligence staff officer, and IO working group representatives to provide a running assessment of the effectiveness of threat information efforts and keeps the operations staff officer and various integrating cells informed.

EVALUATING INFORMATION OPERATIONS

6-14. *Evaluating* is using criteria to judge progress toward desired conditions and determining why the current degree of progress exists (ADRP 5-0). Evaluation is at the heart of the assessment process where most of the analysis occurs. Evaluation helps commanders determine what is working and what is not working, and it helps them gain insights into how to better accomplish the mission.

6-15. During execution, the IO officer works with the intelligence cell and integrating cells to obtain the information needed to determine individual and collective IO effects. Evaluation not only estimates the effectiveness of task execution, but also evaluates the effect of the entire IO effort on the threat, other relevant audiences in the AO, and friendly operations. Evaluation assesses whether IO achieved its scheme of IO and subordinate objectives to support the overall mission.

6-16. In the evaluation phase, two sets of criteria are employed to evaluate progress: MOEs and MOPs. Task execution is evaluated using measures of performance. Task effectiveness, objective attainment, and mission accomplishment are evaluated using measures of effectiveness, which compare achieved results against a baseline. Progress of both MOEs and MOPs is signaled by indicators (see FM 3-13 for IO-specific considerations for each criteria that the commander and staff study when undertaking assessment of effects in the information environment).

6-17. A *measure of effectiveness* is an indicator used to measure a current system state, with change indicated by comparing multiple observations over time (JP 5-0). MOEs help measure changes in conditions, both positive and negative. MOEs are commonly found and tracked in formal assessment plans. MOEs help to answer the question, "Are we doing the right things?" In terms of IO, MOEs chiefly assess changes in the information environment, specifically changes in human behavior. The IO officer is responsible for developing an IO assessment plan as part of the unit's overall formal assessment plan.

6-18. A *measure of performance* is an indicator used to measure a friendly action that is tied to measuring task accomplishment (JP 5-0). MOPs help answer questions such as, "Are we doing things right?" or "Was the action taken?" or "Were the tasks completed to standard?" A MOP confirms or denies that a task has been properly performed. MOPs are commonly found and tracked at all echelons in execution matrixes.

6-19. No direct hierarchical relationship exists between MOPs and MOEs. MOPs do not feed MOEs or combine in any way to produce MOEs. MOPs simply measure the performance of a task; however, these tasks are essential to fulfilling each objective. How MOPs and MOEs relate to each other is driven by unit SOP and the mission or activity being evaluated. For IO, IRC units or staff representatives are responsible for task execution and, in coordination with the IO officer through the IO working group, contribute to MOP development and task assessment.

6-20. In the context of assessment, an *indicator* is an item of information that provides insight into a measure of effectiveness or measure of performance (ADRP 5-0). Indicators take the form of reports from subordinates, surveys, polls, and information requirements. Indicators help to answer the question, "What is the current status of this MOE or MOP?" A single indicator can inform multiple MOPs and MOEs (see table 6-2 for additional information).

Table 6-2. Assessment measures and indicators

	MOE	***MOP***	***Indicator***
Purpose:	Measure attaining an end state condition, achieving an objective, or creating an effect.	Measure task accomplishment.	Provide insight into an MOE or MOP.
Answers:	Are we doing the right things?	Are we doing things right?	What is the status of this MOE or MOP?
Why and What:	Measures *why* (purpose) in the mission statement.	Measures *what* (task completion) in the mission statement.	Information used to make measuring *why* or *what* possible.
Relationship:	No direct hierarchal relationship to MOPs.	No hierarchal relationship to MOEs.	Subordinate to MOEs and MOPs.
Tracking:	Often formally tracked in formal assessment plans.	Often formally tracked in execution matrixes.	Often formally tracked in formal assessment plans.
Level of Challenge:	Typically challenging to choose the appropriate ones.	Typically simple to choose the appropriate ones.	Typically as challenging to select appropriately as the supported MOE or MOP.
MOE measure of effectiveness		MOP measure of performance	

Criteria Development

6-21. IO objectives drive the way in which the staff (IO officer) develops MOEs and MOPs. The unit's mission, commander's intent and guidance, and an understanding of the information environment provide the information required to develop IO objectives. More specifically, objective statements help staffs decide which effects need to be generated in the information environment to achieve the commander's intent. Figure 6-2 shows how to develop the IO objective statement using the effect, target or target audience, action, and purpose (known as ETAP) rubric (see also paragraph 4-39 for details on this rubric).

Note. In the figure 6-2 example, the T stands for *target* because the object of the effect is an entity or object that performs a function for the enemy or adversary, rather than an individual or group selected for influence (for which the T would stand for *target audience*).

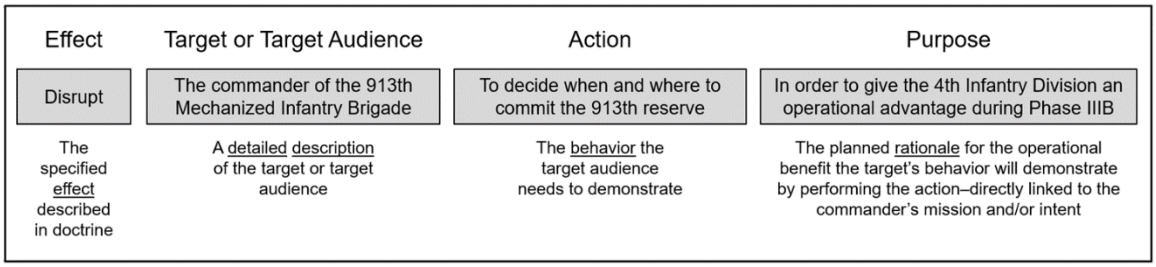

Figure 6-2. Information operations objective statement using effect, target, action, and purpose rubric

Measure of Effectiveness Development

6-22. MOEs measure whether or not units achieved IO objectives successfully—that the effects on the target or target audience produced the desired action or outcome, even if they were not directly caused by planned military action. Typically, the IO officer develops more than one MOE per objective statement to account for randomness, offset disruption or impairment in monitoring the target, and enhance reliability and validity of data. Figure 6-3 on page 6-6 illustrates an MOE statement.

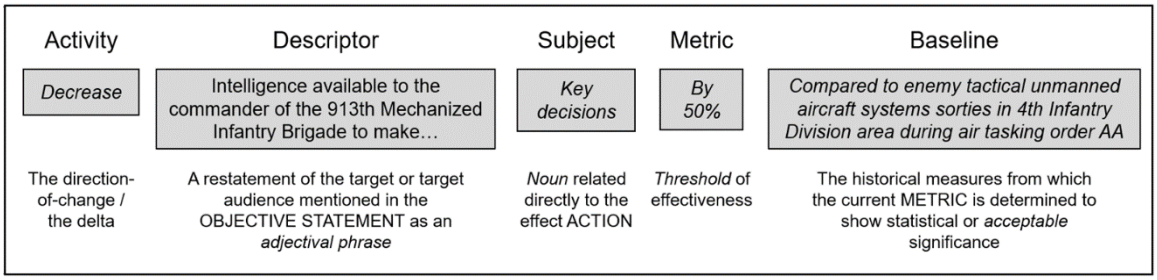

Figure 6-3. Sample measure of effectiveness statement

Measure of Performance Development

6-23. MOPs explain what and how; they specify the activity that IRCs must undertake to create effects in the information environment. MOPs capture the means and medium IRCs will employ, the quantity of effort, and the target. While a given IRC task may have a single MOP, there are typically two or more MOPs. Rarely does a single activity or IRC achieve the desired behavior change. Changing behavior requires both variety and repetition, particularly if such a behavior change needs to be enduring. Figure 6-4 provides an example of how the IO officer, in coordination with IRC representatives, establishes MOPs.

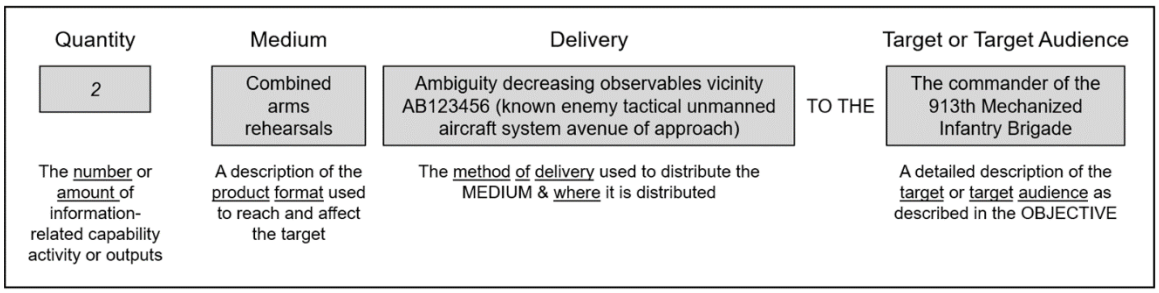

Figure 6-4. Example measure of performance statement

Indicator Development

6-24. Units track the status of MOPs and MOEs using indicators. Indicators are an item of information that provides insight into an MOE or MOP; they are observables or items of information that help the staff determine whether units conduct IRC actions to standard and create the required effect. Using the example MOE statement in figure 6-3, an indicator would be a single enemy tactical unmanned aircraft system sortie. An MOP indicator would be intercepted imagery of the friendly rehearsal captured by the tactical unmanned aircraft system that validates the fact the enemy has observed it.

Logic or Theory of Change

6-25. An important part of the logic of the overall plan is the logic of the IO effort or theory of change in the information environment. Figure 6-5 portrays the relationship among objectives (the change that needs to happen) and MOPs, indicators, and MOEs. The logic of the effort is shown as a relationship among available, selected, and synchronized IRCs and the effects expected over time. While the figure suggests that this logic is generic, it is not. It is specific to every objective and combination of IRCs. Although discussed here as part of assessment, the logic of the IO effort undergirds the scheme of IO (discussed in Chapter 4), reinforcing the cyclical nature of the operations process and the value of post-execution and pre-planning assessments (see also FM 3-13 for a discussion on objectives).

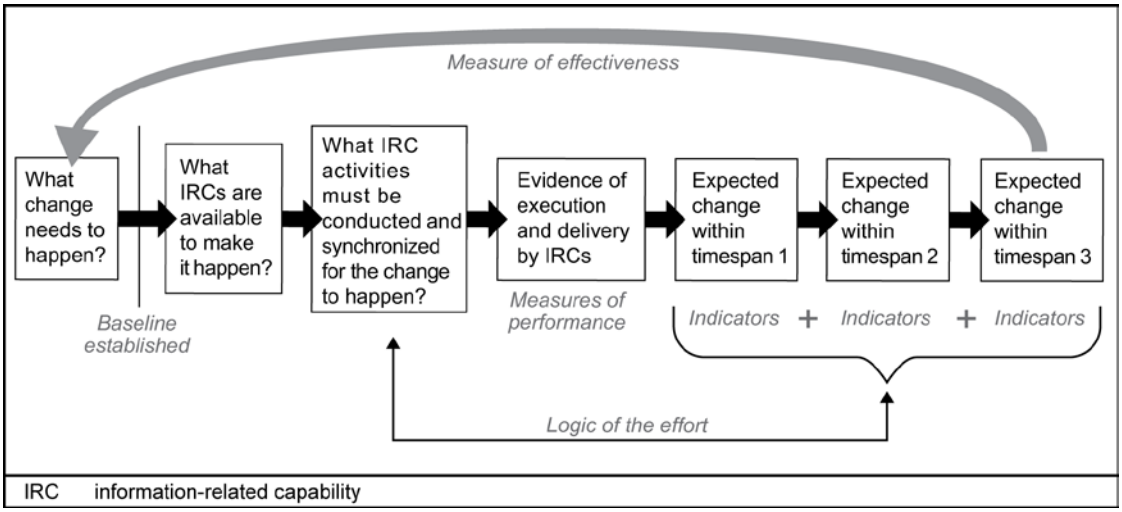

Figure 6-5. Logic flow supporting attainment of an information operations objective

Assessment Products

6-26. Staff assessment products should directly support the commander's requirements, such as deepening understanding of the operational and information environments, measuring progress toward achieving objectives and accomplishing the mission, and informing the commander's intent and guidance. Efficient staffs also develop, tailor, and optimize products to meet the commander's expectations and ways of receiving information. Staffs also tailor products to match the focus or level of assessment. Campaign assessments are substantially fuller or richer in terms of the scope of information presented than is a task assessment.

6-27. As figure 6-5 depicts, achieving IO objectives depends on producing specific effects in the information environment that ultimately cause the enemy or adversary—as well as many intervening variables, actors, or audiences—to change behavior. Assessment, therefore, seeks to verify and explain the change that is or needs to occur—whether through trend analysis or the expected progression from one indicator to another. Figure 6-6 on page 6-8 illustrates several common methods for depicting trends or the status of a given condition in an information environment. Figure 6-7, also on page 6-8, provides a counterinsurgency example that depicts indicator trends supporting an MOE. Figure 6-8 on page 6-9 overlays these trends on a map of the AO.

Note. Staffs can use each of these methods to measure progress among any of the various elements of an IO objective, either singly or in combination: the objective itself or the MOE, MOP, and indicators that support it. Also, effective staffs pair a diagram with additional essential or optional information that facilitates decision making, most importantly the bottom line or "so what."

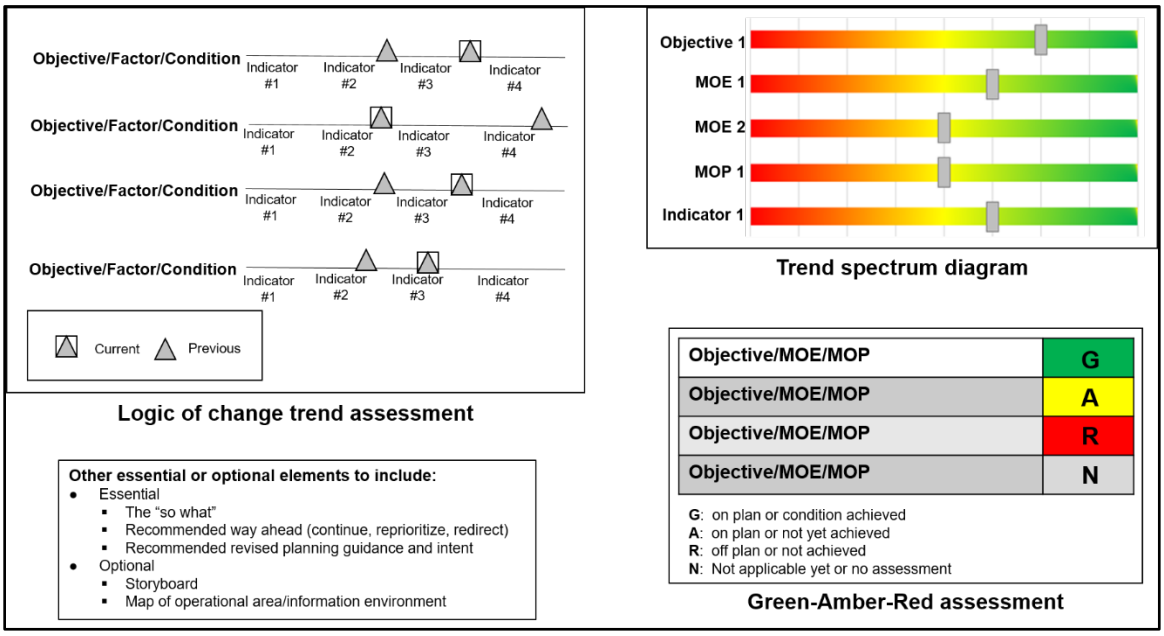

Figure 6-6. Sample assessment product templates

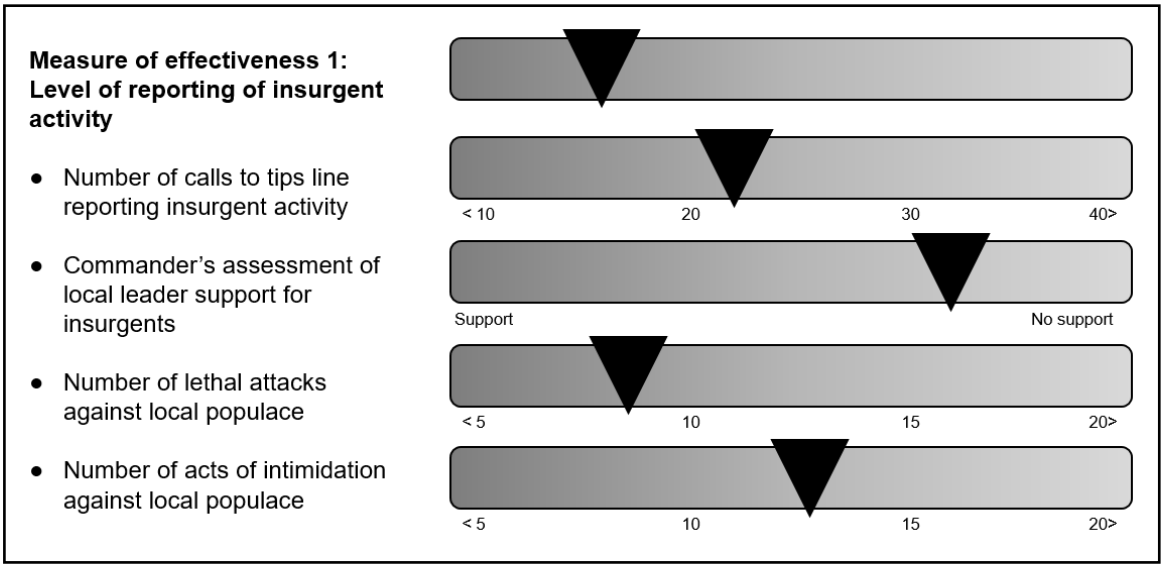

Figure 6-7. Example counterinsurgency measure of effectiveness assessment

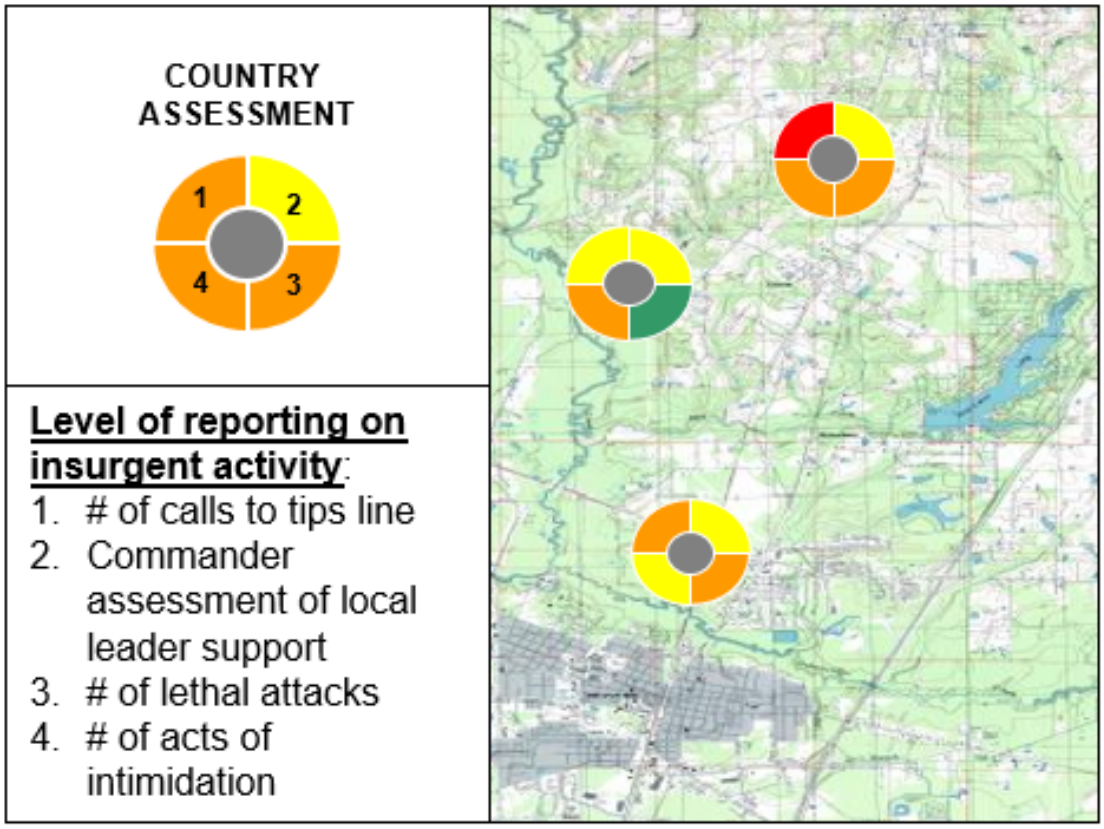

Figure 6-8. Assessment in relation to the area of operations

Adjusting Information Operations

6-28. Monitoring and evaluating are critical activities; however, assessment is incomplete without recommending or directing action or adjustments. Assessment may diagnose problems, but unless it results in recommended adjustments, its use to the commander is limited.

6-29. When developing recommendations, staffs draw from many sources and consider their recommendations within the larger context of the operation. While several ways to improve a particular aspect of the operation might exist, some recommendations could impact other aspects of the operation. As with all recommendations, staffs should address any future implications.

6-30. Based on evaluation, the IO officer adjusts IO to further exploit enemy vulnerabilities, redirects actions yielding insufficient effects, or terminates actions after they have achieved the desired result. The IO officer keeps the operations staff officer and commander informed of IO effects and the impacts they have on friendly and adversary operations.

This page intentionally left blank.

Chapter 7
Information Operations Across Strategic Roles

ARMY STRATEGIC ROLES

7-1. Army IO supports joint IO across the range of military operations and across all operational phases. In planning, a *phase* is a definitive stage of a campaign or operation during which a large portion of the forces and capabilities are involved in similar or mutually supporting activities for a common purpose (JP 5-0). Phasing integrates and synchronizes related activities, thereby enhancing flexibility and unity of effort during execution. Figure 7-1 graphically depicts six phases (0 through 5) in relation to the level of military effort involved (JP 5-0 no longer assigns pre-determined names to each phase) (see FM 3-13 for an overview of IO across the range of military operations).

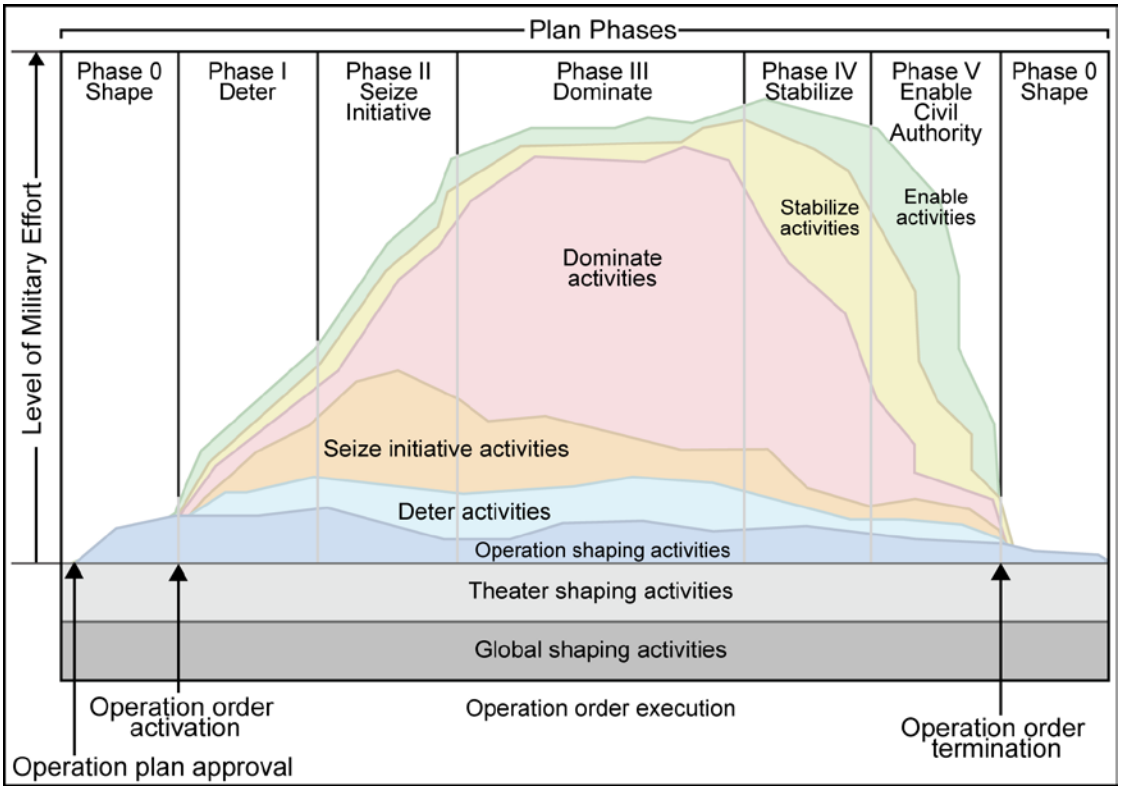

Figure 7-1. Sample phasing model

7-2. The Army recognizes that today's operational environment encompasses the physical areas of the air, land, maritime, space, and cyberspace domains, as well as the information environment (which includes cyberspace) and the electromagnetic spectrum. Thus, the Army now uses a multi-domain approach to operations, integrating joint and Army capabilities and synchronizing actions across all domains to fulfill its strategic roles of shape, prevent, win, and consolidate gains. Figure 7-2 on page 7-2 shows the strategic roles.

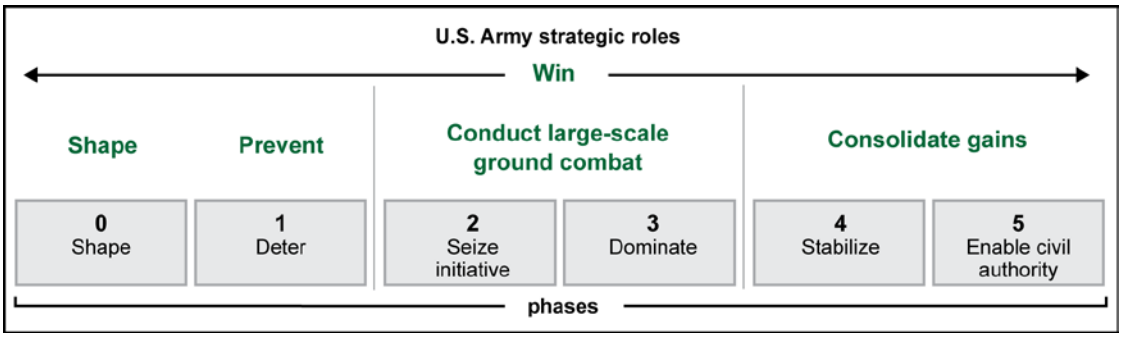

Figure 7-2. Army strategic roles and phases

7-3. IO has three weighted efforts that align with the tasks of decisive action: offense, defense, and stability. The corresponding IO weighted effort for each is attack, defend, and stabilize. IO employs all three weighted efforts in every type of operation (see FM 3-13 for a detailed discussion of the weighted effort). Just because Army forces are executing an offensive operation does not mean they are exclusively weighting IO towards attack. Similarly, when they are conducting defensive operations, they will weight IO to attack, defend, and stabilize simultaneously. The level of each may vary by the type of operation being undertaken, but all three are employed to varying degrees all the time. The same holds true across phases (see figure 7-3). During Phase 1, for example, attack-weighted IO efforts may be conducted alongside defend- and stabilize-weighted efforts. During Phase III, although attack-weighted efforts may be more numerous in comparison to defend and stabilize efforts, all three will be employed.

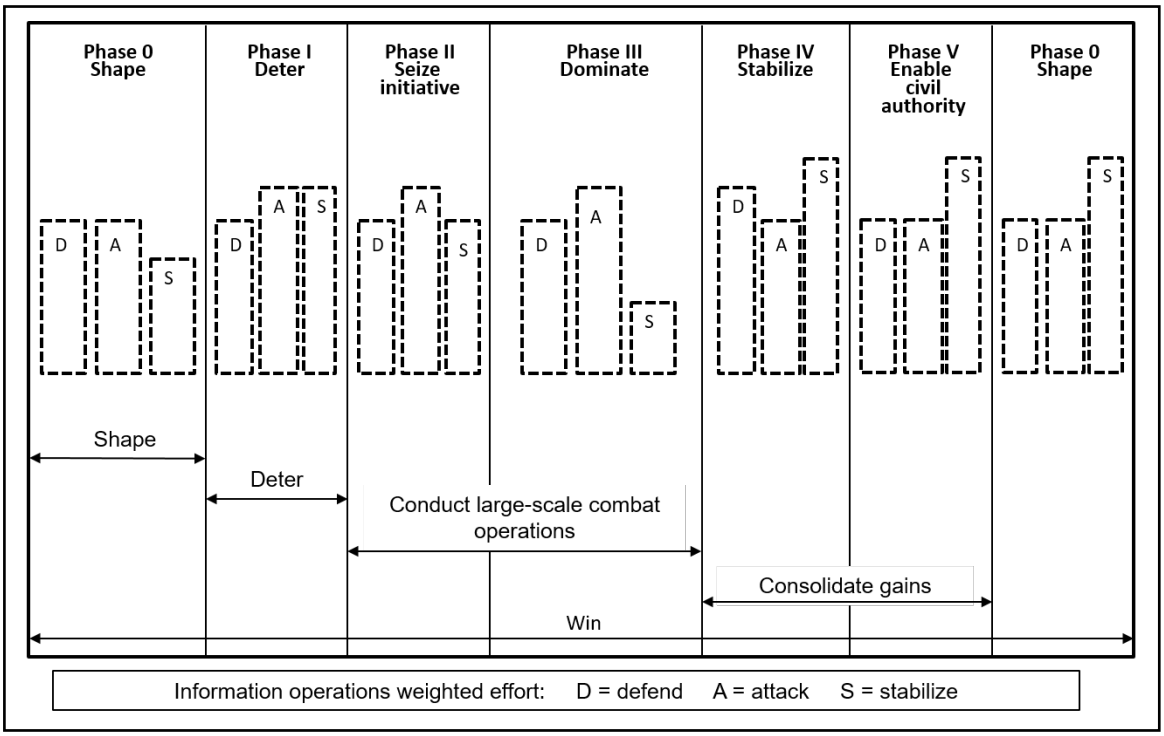

Figure 7-3. IO weighted efforts across phases

SHAPE

7-4. Army operations to shape bring together all the activities intended to promote regional stability and to set conditions for a favorable outcome in the event of a military confrontation. Army operations to shape dissuade adversary activities to achieve regional goals short of military conflict. Shaping activities include enhancing security cooperation and forward presence to promote U.S. interests; developing allied and friendly military capabilities for self-defense and multinational operations; and providing U.S. forces with peacetime and contingency access to a host nation. Regionally aligned and engaged Army forces are essential to achieving objectives that strengthen the global network of multinational partners and prevent conflict. These military operations and activities specifically shape perceptions and influence behaviors of all relevant audiences as necessary to meet U.S. strategic objectives. As such, IO has a significant role in shaping operational environments and may be the decisive line of effort in Phase 0.

7-5. Although shaping operations are ongoing, they are specific to each theater and operational area in which they occur (although effects in one theater may well create effects or achieve objectives in another). The balance of defend, attack, and stabilize IO efforts varies based on the specific operational area, the mission, and the actors or audiences involved. IO considerations or actions during shaping operations may include, but are not limited to, the following:

- Understanding IO implications in the theater campaign plan.
- Embedding IO training and cooperation as part of day-to-day security cooperation.
- Military support to public diplomacy.
- Leveraging available and requested IRCs to achieve cooperative and persuasive influence in the information environment that promotes stability, cooperation, and partnership among allies and potential allies, as well as fosters legitimacy of U.S. and coalition efforts.
- Integrating and synchronizing IRCs to achieve persuasive influence in the information environment that dissuades adversaries or potential adversaries from gaining a malign or disruptive advantage or informs and inoculates the local populace against enemy or adversary propaganda.
- Reviewing contingency plans to ensure requisite IRCs are available in theater and, if not, taking appropriate action to assign or pre-position them or coordinate their proper placement in the time-phased force and deployment data flow.

PREVENT

7-6. Army operations to prevent include all activities to deter an adversary's undesirable actions. These operations are an extension of operations to shape designed to deny the adversary any opportunities to further exploit positions of relative advantage. Army operations to prevent accomplish this by raising the potential costs to adversaries of continuing activities that threaten U.S. interests. Prevent activities are generally weighted toward actions to protect friendly forces, assets, and partners, and to indicate U.S. intent to execute subsequent phases of a planned operation.

7-7. IO considerations during the prevent or deter phase include Phase 0 activities and additionally include, but are not limited to, the following:

- Initiating IO aspects of the theater campaign plan.
- Conducting Soldier and leader engagement with key leaders and influencers specifically to apply persuasive and cooperative influence, and to enhance the legitimacy of U.S. or coalition operations.
- Working in close coordination with unified action partners and host nation IO and IRC forces or units to ensure unity of effort.
- Developing and controlling the narrative and countering the adversary's narrative.
- Military support to public diplomacy.
- Immediately addressing concerns of vulnerable populations to inoculate them against adversary messaging.
- Timely delivery of multiple, complementary messages across numerous platforms that are tied to psychological actions for maximum effect.

- Countering adversarial use of propaganda, misinformation, and disinformation (fake news).
- Increasing frequency and size of exercises and training activities.
- Ensuring that visual information forces (such as combat camera) are embedded in forward troop movements, exercises, and training activities.
- Demonstrating freedom of movement.

CONDUCT LARGE-SCALE GROUND COMBAT

7-8. During large-scale combat operations, Army forces focus on the defeat and destruction of enemy ground forces as part of the joint team. Army forces close with and destroy enemy forces in any terrain, exploit success, and break their opponent's will to resist. Army forces attack, defend, conduct stability tasks, and consolidate gains to attain national objectives. Divisions and corps, which are organized, trained, and equipped to enable subordinate organizations, are the formations central to large-scale combat operations. The ability to prevail in ground combat is a decisive factor in breaking an enemy's will to continue a conflict.

7-9. IO considerations during *seize the initiative* and *dominate* phases include, but are not limited to, the following:

- Employ military deception to mislead the enemy as to the main effort or to otherwise make faulty, poorly timed, or ill-advised decisions that favor Army, joint, or coalition forces.
- Develop messaging that counters the enemy's narrative and neutralizes any bases of support.
- Employ COMCAM and other means to document enemy atrocities or violations of international law, treaties, or norms.
- Employ technical IRCs (such as electronic warfare and offensive cyberspace operations) to attack, disrupt, or degrade enemy command and control.
- Employ technical IRCs (such as electronic warfare and defensive cyberspace operations), information assurance, and OPSEC to protect mission command systems and data.
- Embed media, as appropriate, to provide factual, relevant coverage of Army, joint, or coalition operations.
- Conduct special technical operations against appropriate targets.
- Implement, as appropriate, contingency IO plans and other consequence management activities to respond to incidents or crises.
- Augment multinational arms operations with all available IRCs to ratchet up the intensity of coercive influence applied against the enemy.

CONSOLIDATE GAINS

7-10. Army operations to consolidate gains include activities that promote the permanence of any temporary operational success and set the conditions for a sustainable environment, allowing for a transition of control to legitimate civil authorities. Consolidating gains is an integral and continuous part of armed conflict, and it is necessary for achieving success across the range of military operations. Army forces deliberately plan to consolidate gains during all phases of an operation. Early and effective consolidation activities are a form of an exploitation conducted while other operations are ongoing, and they enable achieving lasting favorable outcomes in the shortest time span. Army forces conduct these activities with unified action partners.

7-11. IO considerations during operations to consolidate gains include, but are not limited to, the following:

- Assisting the legitimate civil authority in shaping themes and messages that increase transparency and bolster legitimacy.
- Addressing or thwarting misinformation or disinformation immediately.
- Providing military support to public diplomacy.
- Explaining continued U.S. or coalition presence and activities.
- Strengthening information capabilities of local partners through training and advisement.
- Employing technical IRCs to support unfettered access to the Internet and other platforms where vital messaging can occur.
- Analyzing the ongoing need for specific IRCs and ensuring they are included in rotation plans.

WIN

7-12. Winning requires commanders to optimize the information element of combat power by conducting IO across all strategic roles and phases. The Army wins when it effectively shapes an operational environment for combatant commanders and when it responds rapidly during crisis with enough combat power to prevent war through deterrence. When required to fight, the Army's ability to prevail in ground combat at any scale becomes a decisive factor in breaking the enemy's will to continue fighting. The Army wins when it defeats an enemy so it can no longer effectively resist, and it agrees to cease hostilities on U.S. terms. In other words, the Army wins when it breaks the enemy's will. To ensure that the military results of combat endure, the Army follows through with its unique scope and scale of capabilities—including those that create effects in the information environment—to consolidate gains and win longstanding outcomes favorable to U.S. interests.

This page intentionally left blank.

Appendix A

Information Operations in Garrison and Training

TRAINING FOCUS

A-1. By its nature, IO can only be oriented or focused against enemies and adversaries abroad. While some elements of IO may be conducted in garrison, they are largely preparatory in nature, ensuring the unit is ready to conduct IO to support named operations. Essential preparation requires training on IO-related tasks at any given level and supporting this training at subordinate levels.

A-2. Units require training to translate doctrine into practice and prepare selected individuals to serve as IO professionals or fulfill IO responsibilities in organizations without an assigned IO officer. One of the most important tasks of IO officers or designated representatives in garrison is to ensure they are proficient at the myriad of IO tasks necessary to successfully conduct IO. They use all the training domains—institutional, operational, and self-development—to ensure this training occurs.

INFORMATION OPERATIONS SELF-DEVELOPMENT TRAINING

A-3. More than the IO officer or designated representative benefits from IO-related self-development training. IO is a commander-led, staff-synchronized process that occurs at all levels of command, across all operational phases, and across the range of military operations. Effective units undertake any self-development that furthers the ability of the commander and staffs to perform their responsibilities related to IO while at home station and with command emphasis. Possible activities and topics for self-development include, but are not limited to—

- Reading books, journals, and other publications related to the conduct of IO, including historical examples, a better understanding of an operational environment and threat, and best practices.
- Gaining a better understanding of operational contracting as well as legal considerations and implications for IO.
- Learning a foreign language and studying relevant cultures, particularly if the unit is regionally aligned.
- Taking related self-developmental courses from the Army Training Requirements and Resources System (ATRRS) that supplement an understanding of any aspect of conducting IO, such as a course on the MDMP.

INFORMATION OPERATIONS OPERATIONAL TRAINING

A-4. Operational training is unit-focused. It comprises individual and collective tasks performed in various settings and prepares individuals, staffs, teams, and units to obtain and sustain peak performance to support their missions. IO tasks are largely individually focused but contribute to a range of mission command collective tasks. Tables A-1 and A-2 on page A-2 and table A-3 on page A-3 portray currently approved individual critical tasks necessary to accomplish IO. Level 10 tasks are for all Soldiers and Department of the Army Civilians to ensure foundational IO knowledge across the force. Level 20 tasks are more specific to Soldiers and Department of the Army Civilians selected to serve as IO representatives or planners on the staff—achieving the additional skill identifier (known as ASI) P4—typically at brigade and below. Level 30 tasks are specific to functional area (known as FA) 30 IO officers (see the Central Army Registry website for tasks and their links).

A-5. Given the increasing importance of the information environment to the range of military operations, units benefit from including at least one IO-related task in their mission-essential task list. Since it supports a specific mission command task, units first consider the task “Conduct Information Operations.” Additionally, units can expect a contested training information environment at their capstone combat training

center (known as CTC) rotation or event. Training in garrison seeks to prepare units for both combat training center events and real-world deployments.

Table A-1. Level 10 information operations individual critical tasks

Task Number	*Task Title*
150-IPO-1000	Define Information Operations
150-IPO-1006	Identify Information Related Capabilities in Support of Unit Operations
150-IPO-1007	Brief Information Operations (IO) as part of Troop Leading Procedures
150-IPO-1008	Interpret a Combined Information Overlay
150-IPO-1009	Identify how Information Operations contributes to the Targeting Process
150-IPO-1010	Define Military Deception (MILDEC)
150-IPO-1011	Communicate Operations Security (OPSEC)
150-IPO-1016	Define the Operational Environment
150-IPO-1017	Define the Information Environment
150-IPO-1027	Conduct a Soldier Leader Engagement

Table A-2. Level 20 information operations individual critical tasks

Task Number	*Task Title*
150-IPO-2006	Integrate Information Related Capabilities (IRCs) in IO Planning
150-IPO-2007	Integrate Information Operations Planning into the Military Decision Making Process (MDMP)
150-IPO-2008	Integrate a Combined Information Overlay into the Intelligence Preparation of the Battlefield (IPB) Process
150-IPO-2009	Integrate Information Operations Planning into the Targeting Process
150-IPO-2010	Integrate Military Deception (MILDEC) into Information Operations Planning
150-IPO-2011	Integrate Operations Security (OPSEC) into Information Operations Planning
150-IPO-2012	Produce an Scheme of Information Operations (Sketch and Statement)
150-IPO-2013	Produce Appendix 15 of an Operations Order (OPORD)
150-IPO-2016	Analyze the Operational Environment
150-IPO-2017	Analyze the Information Environment
150-IPO-2022	Review Measures of Effectiveness and Measures of Performance for Information Operations
150-IPO-2023	Prepare Assessments of Information Operations
150-IPO-2027	Plan a Soldier Leader Engagement (SLE)
150-IPO-2029	Develop a Commander's Mission Narrative
150-IPO-2030	Integrate Intelligence Support into Information Operations Planning
150-IPO-2031	Analyze Adversary Information Operations and Threats in the Information Environment

Table A-3. Level 30 information operations individual critical tasks

Task Number	*Task Title*
150-IPO-3001	Integrate Public Affairs Capabilities into Information Operations Planning
150-IPO-3002	Integrate MISO Capabilities into IO Planning (MISO)
150-IPO-3003	Integrate Cyberspace Operations into IO Planning
150-IPO-3004	Integrate Civil Affairs Capabilities into Information Operations Planning
150-IPO-3005	Integrate Electronic Warfare Capabilities into IO Planning
150-IPO-3006	Integrate Other Information Related Capabilities (IRCs) into Information Operations Planning
150-IPO-3007	Integrate Information Operations Planning into the Military Decision Making Process (MDMP)
150-IPO-3008	Produce a Combined Information Overlay
150-IPO-3009	Integrate Information Operations into the Targeting Process
150-IPO-3010	Develop Military Deception (MILDEC) Plans in Support of Operations
150-IPO-3011	Integrate OPSEC into Information Operations Planning
150-IPO-3012	Produce an Information Operations (IO) Scheme of Support (Sketch and Statement)
150-IPO-3013	Produce Appendix 15 (Information Operations) of an Operations Order
150-IPO-3015	Integrate Special Technical Operations into Information Operations Planning
150-IPO-3016	Analyze the Operational Environment
150-IPO-3017	Analyze the Information Environment
150-IPO-3018	Analyze a Culture
150-IPO-3021	Integrate the Stability Assessment Framework into IO Planning
150-IPO-3022	Develop Measures of Performance and Measures of Effectiveness (MOE/MOP)
150-IPO-3023	Conduct Assessment of Information Operations
150-IPO-3026	Coordinate Information Operations with Unified Action Partners and Multi-National Partners
150-IPO-3027	Integrate Soldier and Leader Engagements into Information Operations Planning
150-IPO-3028	Conduct an Information Operations Working Group
150-IPO-3030	Integrate Intelligence Support into Information Operations Planning
150-IPO-3031	Counter Adversary Information Operations and Threats in the Information Environment
150-IPO-3032	Develop a Communication Strategy
150-IPO-3033	Conduct FA30 Professional Development and Career Management
150-IPO-3035	Coordinate Resourcing for Information Operations and Request For Forces (RFF)
150-IPO-3036	Direct Imagery Collection in Support of IRCs and Commander's Themes and Messages (Using Combat Camera and Other Resources)

INFORMATION OPERATIONS INSTITUTIONAL TRAINING

A-6. Joint and Army institutional courses that are IO-specific or related are numerous. They are offered by the U.S. Information Operations Proponent Office, the 1st Information Operations Command (Land), the 3-124th IO Battalion, Vermont Army National Guard, and the Joint Forces Staff College. All Army courses can be found at the ATRRS website. Information on joint courses can be found at the links provided in their descriptions.

INFORMATION OPERATIONS QUALIFICATION OR PREPARATION COURSES

A-7. Two courses prepare personnel to serve as the staff IO planner or officer. The Tactical Information Operations Planner Course prepares noncommissioned officers and officers to fulfill IO responsibilities at

brigade and below levels. The Functional Area FA 30 (IO) Qualification Course prepares officers to serve in IO billets at division and higher. The FA 30 (IO) Qualification Course is taught by the Information Operations Proponent Office, Fort Leavenworth, Kansas (for Regular Army and Reserve Component officers) and by the 3-124th IO Battalion, Vermont Army National Guard (Reserve Component officers). Other IO preparatory courses listed are provided by the 1st IO Command and the Joint Forces Staff College.

Functional Area 30 (IO) Qualification Course (FA30QC)

A-8. The Functional Area 30 (IO) Qualification Course is a twelve-week credentialing course for officers assessed as FA30s. The course employs guest speakers and experts from academia, industry, government, military, and current IO officers. The students learn how to integrate and synchronize IRCs, lead IO working groups, and develop the MDMP-related products to serve as IO officers at division and higher echelons. Students participate in an end of course exercise to assess each student's ability to plan, execute, assess, and adapt tactics, techniques, and procedures throughout unified land operations (see ATRRS school code 150 and course code 2G-FA30 for enrollment procedures and course information).

Functional Area 30 (IO) Qualification Course (Reserve Component)

A-9. The Information Operations Qualification Course (IOQC) (Reserve Component) is a 9-month, 3-phase course taught by the 3-124th IO Battalion, Vermont Army National Guard. Phase 1 is approximately 40 hours of self-paced distance learning. Phase 2 is 28 four-hour period unit training assemblies (known as UTAs) held once per weeknight for four hours over a secure Defense Connect Online (known as DCO) connection where students collaborate with fellow students and instructors. Students encounter a workload similar to an online master's degree program, including presentations, papers, readings, exercises, and tests. Phase 2 requires a significant time commitment beyond the four hours per week of collaborative online learning. Phase 3 is a 15-day (13 days of instruction plus 2 travel days) resident exercise held at Camp Johnson, Vermont (see ATRRS school code 1030 and course code 2G-FA30 for enrollment procedures and prerequisites).

Tactical Information Operations Planner Course

A-10. The Tactical IO Planner Course (known as TIOPC) consists of a combination of distance learning and one week of resident instruction. The course prepares students to conduct tactical IO planning, execution, and assessment. The course addresses all IO elements and activities, focusing on the synchronization and coordination of—

- Operations security.
- Military information support operations.
- Military deception.
- Electronic warfare.
- Physical destruction.
- Public affairs.
- Civil-military operations.

Graduates earn the P4 additional skill identifier (see school code 1030, course code 150-9E-SI/ASIP4/ 950-ASIP4 in ATRRS for enrollment procedures and prerequisites).

Note. The Tactical IO Planner Course is being revised to have a common program of instruction with the Information Operations Capabilities, Applications, and Planning course. When completed, the revised course will be titled the Army Information Operations Planner's Course (known as AIOPC).

Information Operations Capabilities, Applications, and Planning Course

A-11. The Information Operations Capabilities, Applications, and Planning (known as IOCAP) course aims to teach students to integrate IO into staff planning to support unit (Army) operations. The course curriculum

details IO; the role of the IO planner; integration of IRCs into the MDMP (focusing on mission analysis and COA development); the IO planner's participation in other staff processes such as IPB, targeting, and assessment; and the importance of cultural considerations in IO. This course emphasizes integrating, synchronizing, and coordinating IRCs to shape the information environment to support military operations. The training is entirely classroom-based and instruction is provided by the 1st IO Command (Land). Training is conducted at the collateral secret level for resident courses and at the unclassified level for mobile training teams. Graduates are eligible for the P4 additional skill identifier. Training is recommended for IO planners, intelligence specialists to support IO, and IRC representatives to support IO (see ATRRS school code 024, course code 15-F30 IOCAP (MC) for course information and prerequisites).

Note. The Information Operations Capabilities, Applications, and Planning course is being revised to have a common program of instruction with the Tactical IO Planner Course (known as TIOPC). When completed, the revised course will be titled the Army Information Operations Planner's Course (AIOPC).

Information Operations Fundamentals Course

A-12. The IO Fundamentals Course (known as IOFC), also provided by the 1st IO Command, is for Soldiers, Department of Defense (DOD) civilians, and contractors who require an understanding of the doctrine and principals associated with Army IO but are not expected to be IO planners. The course curriculum covers IO; the role of the IO planner; integrating IRCs into the MDMP (focus on mission analysis and course of action development); the IO planner's participation in other staff processes such as IPB, targeting, and assessment; and the importance of cultural considerations in information operations. The training is entirely classroom based and uses lecture; discussion; problem-based or experiential learning-based facilitation; and performance-based practical exercises. The training is conducted at the unclassified level and is only available in a mobile training team (known as MTT) format (see ATRRS school code 024, course code IOFC for course information and prerequisites).

Joint Information Operations Planners' Course

A-13. The Joint Information Operations Planners' Course (JIOPC) aims to educate and train military students between the ranks of 0-4 through 0-6 and DOD civilian equivalents to plan, integrate, and synchronize IO into joint operational-level plans and orders. The school accomplishes this by combining distance learning, in-residence class presentations, guest lectures, case studies, and practical exercises in a joint seminar environment. Specifically, the course focuses on the following six learning areas:

- Adaptive planning and execution (known as APEX) system.
- Joint intelligence preparation of the operational environment (known as JIPOE).
- IO planning.
- Interagency planning and coordination.
- Military deception.
- Operations security.

More information can be found at http://jfsc.ndu.edu/Academics/Joint-C2-Information-Operations-School-JC2IOS/Information-Operations-Division/JIOPC.

Related Training

A-14. The following courses augment and complement IO-specific training. This list is not exhaustive. New courses may arise that provide IO personnel additional specialized knowledge and skills that enable them to fulfill their responsibilities with greater precision and effectiveness. The IO proponent, through various communication platforms—most especially the FA 30 Community page on Army Career Tracker—provides updates on training for IO personnel. Ultimately, training attendance is command-driven and a function of time and budget considerations.

1st Information Operations Command (Land) Courses

A-15. The 1st IO Command (Land) provides training in a number of areas. These include military deception, cyberspace operations, and electronic warfare integration. Information about the first three courses can be found in ATRRS under school code 024. Information about the OPSEC course is found on U.S. Army OPSEC Support Element's (known as OSE) website on Army Knowledge Online.

Military Deception Planners Course

A-16. The Military Deception Planners Course (known on MDPC) consists of 40-hours of formal classroom instruction and a hands-on practical exercise. The training follows the five-phase military deception planning cycle (Capability Development, Assessment Phase, Planning Phase, Execution Phase, and Termination Phase). The instruction covers MILDEC policy, doctrine, terminology, fundamentals, and principles; and time proven tactics, techniques, and procedures. Students receive eight hours of formal lecture, with the remaining 32 hours devoted to walking each participant through the entire deception cycle following a realistic training scenario. Each day, students view a video of a different historical case study to reinforce learning objectives. All students receive a bound student guide, key consideration book, and a copy of the Department of the Army Military Deception Planners' Guide (see ATRRS school code 024, course code 15-F30 MDPC (MC) for course information and prerequisites).

Electronic Warfare Integration Course

A-17. The Electronic Warfare Integration Course (known as EWIC) course teaches students to integrate, synchronize, and coordinate EW planning and execution with IO. The course introduces students to EW concepts, fundamentals, doctrine, and capabilities in the DOD. This introduction covers the electromagnetic spectrum, effects on radio and radars in the electromagnetic spectrum arena, EW systems and capabilities, electromagnetic spectrum management, EW emerging technologies, and electronic systems populating an operational environment. The training includes an overview of current and emerging DOD EW doctrine, Army EW organization, EW platforms and missions, intelligence support to EW, and duties and responsibilities of an EW officer operating within a theater-level EW coordination cell (see ATRRS school code 024, course code 15-F30 EWIC (MC) for course information and prerequisites).

Military Information Support Operations Integration Course

A-18. The MISO Integration Course (known as MISOIC) introduces IO planners and IO capability specialists to the concepts, fundamentals, doctrine, and capabilities of Army MISO. Through 40 hours of platform instruction and hands-on practical exercises, the MISO Integration Course provides IO planners and IO capability specialists with an overview of MISO roles and responsibilities; key terms and definitions; the history of MISO; MISO task organization; key equipment and capabilities; MISO programs and authorities; the seven-phase MISO development process; MISO's role in countering adversary information; a discussion of several MISO case studies; and, most importantly, the integration of MISO into IO planning using the MDMP and the targeting processes. The MISO Integration Course is not a MISO qualification course, nor does it provide training on how to conduct MISO. The training is conducted at the secret level (see ATRRS school code 024, course code 15-F30 MISOIC (MC) for course information and prerequisites).

Department of the Army OPSEC Program Manager/Officer Course

A-19. This course is offered as a mobile training team (known as MTT) of the 1st Battalion, 1st IO Command (Land) for units or installations to certify multiple OPSEC program managers or officers (25 through 30 personnel). The course is tailored to the Army units requesting the course and taught by two instructors from the OPSEC Support Element. The course prepares Army OPSEC program managers and program officers to provide OPSEC planning and analysis support to their commanders; to develop and implement an OPSEC program in accordance with AR 530-1; to integrate OPSEC into mission planning; and to plan and conduct OPSEC assessments. More information can be found at https://www.us.army.mil/suite/grouppage/92123.

Cyberspace Operations Integration Course

A-20. The Cyberspace Operations Integration Course (known as COIC) is a 40-hour course that prepares IO planners to integrate, synchronize, and coordinate cyberspace operations with other IRCs to support the commander's objectives. The course focuses on understanding cyber threats, vectors, and tactics, techniques, and procedures (known as TTP); applying cyberspace operations policy, doctrine, and authorities; understanding cyber organizations roles, relationships, and responsibilities; applying combatant command planning frameworks; coordinating and integrating intelligence support to cyberspace operations; coordinating the integration of cyberspace targets into the targeting process; identifying key infrastructure, terrain, and information; integrating cyberspace operations to support IO objectives; deconflicting cyberspace operations with other IRCs; conducting cyberspace-focused risk assessments; conducting operational assessments; coordinating cyberspace operations effects requests; and developing applicable orders, plans, and annexes (see ATRRS school code 024, course code 15-F30 COIC (MC).

Joint Forces Staff College Courses

A-21. The Joint Forces Staff College, through its Joint Command and Control and Information Operations School (known as JC2IOS), offers IO-augmenting courses from a joint perspective. These courses cover MILDEC, OPSEC, and cyberspace operations. More information about these courses can be found at the Joint Forces Staff College website for each specific course at http://jfsc.ndu.edu/Academics/Joint-C2-Information-Operations-School-JC2IOS. The Joint Forces Staff College website offers additional links and information for joint courses.

Joint Military Deception Training Course

A-22. This course educates and trains selected military students between the grades of E-6 through E-9, grades O-3 through O-6, DOD civilian equivalents, and designated contractors assigned to plan, execute, or support joint MILDEC. Course graduates will demonstrate basic-level proficiency in planning, conducting, and assessing joint MILDEC and deception in support of operations security (known as DISO) across the range of military operations and in accordance with applicable doctrine, policy, and authorities. This course is taught by the IO Division.

Defense Operations Security Planner Course

A-23. This one-week course educates and trains selected military students between the grades of E-6 through E-9, grades O-3 through O-6, DOD civilian equivalents, and designated contractors assigned as operations security planners, J-5 or joint planning group planners, and OPSEC program managers. Course graduates will learn to effectively plan, integrate, conduct, and assess joint OPSEC at the joint or operational level across the range of military operations and in accordance with applicable doctrine, policy, and authorities. Graduates will also learn to enhance corporate knowledge of vulnerabilities associated with operations and plans for the joint warfighter. This course is taught by the IO Division.

Joint Command, Control, Communications, Computers and Intelligence/Cyber Staff and Operations Course

A-24. The Joint Command, Control, Communications, Computers and Intelligence/Cyber Staff and Operations Course (known as JC4ICSOC) is a three-week operational level resident course sponsored by the Joint Staff J-6. The mission of this course is to educate and train joint command, control, communications, computers, and intelligence (C4I) decision makers. These personnel work in C4I and cyberspace concepts in the joint, interagency, and multinational environments in the DOD's organization. Graduates learn how to support the C4I process, manage joint C4I systems, and operate current joint C4I systems. Students are required to demonstrate their learning by successfully completing an academic paper, a classroom paper presentation, and an end of course examination. This course is taught by the C4I Division.

Other Courses

A-25. The following courses augment and complement IO-specific training. This list is not exhaustive.

Red Team Leader Course

A-26. This 18-week, 4-day course provides students instruction in the following four areas: introspection and self-reflection, groupthink mitigation, fostering cultural empathy, and applied critical thinking. It is taught by the University of Foreign Military and Cultural Studies at Fort Leavenworth, Kansas at the secret level. Shorter versions of the course are available (see ATRRS school code 159, course code 9E-SI/ASI7G/920-ASI7G).

U.S. Army Special Technical Operations Planner Course

A-27. In this 40-hour course, students learn U.S. Army and joint special technical operations (STO) doctrine, organizations, employment, and tools. The course is based at Fort Sill, Oklahoma but is taught via a mobile training team (known as MTT) at requesting locations worldwide. It requires clearance at the top secret and sensitive compartmented information-levels (see ATRRS school code 061 and course code 2E-F280/250-F69 (RP).

Special Operations Military Deception Planners Course

A-28. This 91-hour course presents the core MILDEC tasks and knowledge to execute the deception cycle as the MILDEC officer of a special operations force staff or conventional force staff during conduct of an irregular warfare scenario in a problem-centered active learning environment. The training is conducted at the top-secret level at the John F. Kennedy Special Warfare Center and School, Fort Bragg, North Carolina (see ATRRS school code 331, and course code 2E-F286/011-F119).

Information Environment Advanced Analysis Course

A-29. The 40-hour, joint-certified, contractor-delivered Information Environment Advanced Analysis (known as IEAA) Course equips students working in joint settings with concepts, techniques, and constructs that will enable them to anticipate, sustain, and seize the initiative in the information environment. It is sponsored by the Office of the Undersecretary of Defense for Intelligence (known as OUSD/I).

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AFR	Air Force Reserve
AO	area of operations
ASCC	Army Service component command
ATP	Army techniques publication
CAO	civil affairs operations
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CCIR	commander's critical information requirement
CEMA	cyberspace electromagnetic activities
CIO	combined information overlay
COA	course of action
COG	center of gravity
COMCAM	combat camera
DA	Department of the Army
DLAR	Defense Logistics Agency Regulation
DOD	Department of Defense
DODD	Department of Defense directive
EEFI	essential element of friendly information
EW	electronic warfare
FM	field manual
IJSTO	integrated joint special technical operations
IO	information operations
IPB	intelligence preparation of the battlefield
IRC	information-related capability
JP	joint publication
MCO	Marine Corps order
MDMP	military decisionmaking process
MILDEC	military deception
MISO	military information support operations
MOE	measure of effectiveness

MOP	measure of performance
OPNAVINST	Chief of Naval Operations instruction
OPSEC	operations security
PA	public affairs
PIR	priority intelligence requirement
PPP	presence, profile, and posture
SLE	Soldier and leader engagement
TIOG	Theater Information Operations Group
U.S.	United States

SECTION II – TERMS

assessment

Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. (JP 3-0)

commander's critical information requirement

An information requirement identified by the commander as being critical to facilitating timely decision making. (JP 3-0)

commander's intent

A clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned. (JP 3-0)

cyberspace

A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

cyberspace electromagnetic activities

The process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations. (ADRP 3-0)

cyberspace operations

The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)

electronic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-13.1)

essential element of friendly information

(Army) A critical aspect of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection. (ADRP 5-0)

evaluating

Using criteria to judge progress toward desired conditions and determining why the current degree of progress exists. (ADRP 5-0)

fires

The use of weapon systems or other actions to create specific lethal or nonlethal effects on a target. (JP 3-09)

indicator

(Army) In the context of assessment, an item of information that provides insight into a measure of effectiveness or measure of performance. (ADRP 5-0)

information environment

The aggregate of individuals, organizations, and systems that collect, process, dissseminate, or act on information. (JP 3-13)

information operations

The integrated employment, during military operations, of information-related capabilities 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)

information-related capability

A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. (JP 3-13)

information requirement

Any information elements the commander and staff require to successfully conduct operations. (ADRP 6-0)

intelligence

The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. (JP 2-0)

intelligence estimate

The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 2-0)

intelligence preparation of the battlefield

The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. (ATP 2-01.3)

intelligence requirement

A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (JP 2-0)

measure of effectiveness

An indicator used to measure a current system state, with change indicated by comparing multiple observations over time. (JP 5-0)

measure of performance

An indicator used to measure a friendly action that is tied to measuring task accomplishment. (JP 5-0)

message

A narrowly focused communication directed at a specific audience to support a specific theme. (JP 3-61)

military information support 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 in a manner favorable to the originator's objectives. (JP 3-13.2)

mission command

(Army) The exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations. (ADP 6-0)

monitoring

Continuous observation of those conditions relevant to the current operation. (ADRP 5-0)

narrative

Overarching expression of context and desired results. (JDN 2-13)

operation

A sequence of tactical actions with a common purpose or unifying theme. (JP 1)

operational approach

A broad description of the mission, operational concepts, tasks, and actions required to accomplish the mission. (JP 5-0)

operational environment

A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

operations security

A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. (JP 3-13.3)

phase

In planning, a definitive stage of a campaign or operation during which a large portion of the forces and capabilities are involved in similar or mutually supporting activities for a common purpose. (JP 5-0)

physical security

That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 3-0)

priority intelligence requirement

An intelligence requirement that the commander and staff need to understand the threat and other aspects of the operational environment. (JP 2-01)

public affairs

Communication activities with external and internal audiences. (JP 3-61)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ADP 5-0)

Soldier and leader engagement

Interpersonal Service-member interactions with audiences in an area of operations. (FM 3-13)

spectrum management operations

The interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. (FM 6-02)

target

An entity or object that performs a function for the adversary considered for possible engagement or other action. (JP 3-60)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

terrain analysis

The collection, analysis, evaluation, and interpretation of geographic information on the natural and man-made features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. (JP 2-03)

theme

Unifying idea or intention that supports the narrative and is designed for broad application to achieve specific objectives. (JDN 2-13)

unified land operations

Simultaneous offensive, defensive, and stability or defense support of civil authorities tasks to seize, retain, and exploit the initiative to shape the operational environment, prevent conflict, consolidate gains, and win our Nation's wars as part of unified action. (ADRP 3-0)

This page intentionally left blank.

References

All URLs accessed on 14 September 2018.

REQUIRED PUBLICATIONS

Readers require these publications for fundamental concepts, terms, and definitions.

DOD Dictionary of Military and Associated Terms. August 2018.

ADP 1-02. *Terms and Military Symbols.* 14 August 2018.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

DEPARTMENT OF DEFENSE PUBLICATIONS

DOD issuances are available at http://www.esd.whs.mil/DD/DoD-Issuances/.

DODD 3600.01. *Information Operations (IO).* 2 May 2013.

DODD 5205.07. *Special Access Program (SAP) Policy*. 1 July 2010.

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/.

JDN 2-13. *Commander's Communication Synchronization*. 18 December 2013.

JP 1. *Doctrine for the Armed Forces of the United States.* 25 March 2013.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 5 July 2017.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment.* 21 May 2014.

JP 2-03. *Geospatial Intelligence in Joint Operations.* 5 July 2017.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-09. *Joint Fire Support.* 12 December 2014.

JP 3-12. *Cyberspace Operations*. 8 June 2018.

JP 3-13. *Information Operations*. 27 November 2012.

JP 3-13.1. *Electronic Warfare*. 8 February 2012.

JP 3-13.2. *Military Information Support Operations.* 21 November 2014.

JP 3-13.3. *Operations Security*. 6 January 2016.

JP 3-13.4. *Military Deception*. 14 February 2017.

JP 3-57. *Civil-Military Operations.* 9 July 2018.

JP 3-60. *Joint Targeting*. 31 January 3013.

JP 3-61. *Public Affairs*. 17 November 2015.

JP 5-0. *Joint Planning.* 16 June 2017.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil.

ADP 5-0. *The Operations Process.* 17 May 2012.

ADP 6-0. *Mission Command*. 17 May 2012.

ADRP 1. *The Army Profession*. 14 June 2015.

ADRP 3-0. *Operations*. 6 October 2017.

ADRP 5-0. *The Operations Process*. 17 May 2012.

ADRP 6-0. *Mission Command*. 17 May 2012.

AR 190-13. *The Army Physical Security Program*. 25 February 2011.

AR 190-16/OPNAVINST 5530.15A/AFR 207-4/MCO 5500.13A/DLAR 5710.4. *Multi-Service Doctrine for Physical Security*. 31 May 1991.

AR 530-1. *Operations Security*. 26 September 2014.

ATP 1-05.03. *Religious Support and External Advisement*. 3 May 2013.

ATP 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace*. 10 November 2014.

ATP 2-22.9. *Open-Source Intelligence (U)*. 30 June 2017.

ATP 2-33.4. *Intelligence Analysis*. 18 August 2014.

ATP 3-05.20. *Special Operations Intelligence*. 3 May 2013.

ATP 3-60. *Targeting*. 7 May 2015.

ATP 5-0.1. *Army Design Methodology*. 1 July 2015.

ATP 6-02.40. *Techniques for Visual Information Operations*. 27 October 2014.

FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.

FM 3-13. *Information Operations*. 6 December 2016.

FM 3-14. *Army Space Operations*. 19 August 2014.

FM 3-39. *Military Police Operations*. 26 August 2013.

FM 3-57. *Civil Affairs Operations*. 31 October 2011.

FM 3-61. *Public Affairs Operations*. 1 April 2016.

FM 6-0. *Commander and Staff Organization and Operations*. 5 May 2014.

FM 6-02. *Signal Support to Operations.* 22 January 2014.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

OTHER PUBLICATIONS

Paul, Christopher, Jessica Yeats, Colin P. Clarke, Miriam Matthews, and Lauren Skrabala. *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners*. Santa Monica, CA: RAND Corporation, 2015. http://comm.eval.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=45b2d092-0c76-4a81-a13a-f1f0087c2dce.

Tunnicliffe, Ian, and Steve Tatham. “Social Media—The Vital Ground: Can We Hold It?” in *The Letort Papers* (Carlisle, PA: U.S. Army War College Press, 2017). Available at https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1349.

WEBSITES

U.S. Army. “Army Training Requirements and Resources System (ATRRS).” https://www.atrrs.army.mil/atrrs2.aspx.

U.S. Army. “Central Army Registry (CAR).” https://atiam.train.army.mil/catalog/dashboard.

Joint Forces Staff College. “Home Page of the Joint Forces Staff College (JFSC).” http://jfsc.ndu.edu/.

RECOMMENDED READINGS

The listing on the following pages is not exhaustive but offers a starting point for IO officers, staff officers in general, and commanders who seek to augment their knowledge of IO.

CENTER FOR ARMY LESSONS LEARNED (CALL) PUBLICATIONS

Handbook 14-16. *Staff Officer's Quick Reference Guide: Lessons and Best Practices.* Version 3, September 2014. https://call2.army.mil/toc.aspx?document=7279.

Handbook 15-03. *Information Operations Quick Reference Guide: Lessons and Best Practices.* February 2015. https://call2.army.mil/toc.aspx?document=7283.

Handbook 15-06. *MDMP: Lessons and Best Practices.* March 2015. https://call2.army.mil/toc.aspx?document=7288.

Handbook 15-15. *Unified Action Partners' Quick Reference Guide: Lessons and Best Practices.* September 2015. https://call2.army.mil/toc.aspx?document=7309.

Handbook 16-15. *The Electronic Warfare Smartbook.* May 2016. https://call2.army.mil/toc.aspx?document=7383.

Handbook 17-09. *Russian New Generation Warfare.* Version 2.1, April 2017. https://call2.army.mil/toc.aspx?document=7434.

RAND PUBLICATIONS

Helmus, Todd, Christopher Paul, and Russell Glenn. *Enlisting Madison Avenue: The Marketing Approach to Earning Popular Support in Theaters of Operation*. RAND Corporation, 2007. https://www.rand.org/pubs/monographs/MG607.html.

Marcellino, William, Meagan L. Smith, Christopher Paul, and Lauren Skrabala. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1742.html.

Paul, Christopher. *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Worked Example*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR809z4.html.

Paul, Christopher. "On Strategic Communication Today: Enhancing U.S. Efforts to Inform, Influence, and Persuade," *Parameters* 46, no. 3 (Autumn 2016): 87-97. http://www.rand.org/pubs/external_publications/EP66761.html.

Paul, Christopher and William Marcellino. *Dominating Duffer's Domain: Lessons for the U.S. Army Information Operations Practitioner*. Santa Monica, CA: RAND Corporation, 2017. http://www.rand.org/pubs/research_reports/RR1166z1.html.

Paul, Christopher, and Miriam Matthews. *The Russian "Firehose of Falsehood" Propaganda Model: Why it Might Work and Options to Counter It*. Rand Corporation, 2016. https://www.rand.org/pubs/perspectives/PE198.html.

Paul, Christopher, Jessica Yeats, Colin P. Clarke, and Miriam Matthews. *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: An Annotated Reading List*. Santa Monica, CA: RAND Corporation, 2015. http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR809z3/RAND_RR809z3.pdf.

Paul, Christopher, Jessica Yeats, Colin P. Clarke, and Miriam Matthews. *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference*. Santa Monica, CA: RAND Corporation, 2015. http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR809z1/RAND_RR809z1.pdf.

Paul, Christopher, Jessica Yeats, Colin P. Clarke, Miriam Matthews, and Lauren Skrabala. "Assessing and Evaluating DoD Inform, Influence, and Persuade Efforts: Guidance for Practitioners," *IO Sphere* (Fall 2015): 43-49. http://www.rand.org/pubs/external_publications/EP50917.html.

Porche, Isaac R., III, Caolionn O'Connell, John S. Davis II, Bradley Wilson, Chad C. Serena, Tracy C. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, and Michael Vasseur. *Cyber Power Potential of the Army's Reserve Component*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1490.html.

Porche, Isaac R., III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick. *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*. Santa Monica, CA: RAND Corporation, 2017. http://www.rand.org/pubs/research_reports/RR1600.html.

FOREIGN MILITARY STUDIES OFFICE PUBLICATIONS

The Foreign Military Studies Office (FMSO) provides a comprehensive Information Warfare/ Information Operations reading list at https://community.apan.org/wg/tradoc-g2/fmso/

OTHER PUBLICATIONS

Cialdini, Robert B., Ph.D. *Influence: The Psychology of Persuasion*. New York: Collins Business, 2007.

Corman, Steven R., Angela Trethewey, and Bud Goodall. *A 21st Century Model for Communication in the Global War of Ideas: From Simplistic Influence to Pragmatic Complexity*. Tempe, AZ: Consortium for Strategic Communication, Arizona State University, 2007. Available at http://csc.asu.edu/wp-content/uploads/pdf/114.pdf.

Gladwell, Malcolm. *The Tipping Point: How Little Things Can Make a Big Difference*. Boston: First Back Bay, 2002. First published in 2000 by Little, Brown and Company (Boston).

Heath, Chip, and Dan Heath. *Made to Stick: Why Some Ideas Survive and Others Die*. New York: Random House, 2008.

MacKay, Andrew, and Steve Tatham. *Behavioral Conflict: Why Understanding People and Their Motivations Will Prove Decisive in Future Conflict*. Essex, United Kingdom: Military Studies Press, 2011.

Montagu, Ewen. *The Man Who Never Was: World War II's Boldest Counterintelligence Operation*. Annapolis, MD: Naval Institute Press, First Bluejacket Books, 2001. First published 1953 by Oxford University Press (New York).

Nissen, Thomas Elkjer. "Narrative Led Operations: Put the Narrative First." *Small Wars Journal* (October 2012). http://smallwarsjournal.com/jrnl/art/narrative-led-operations-put-the-narrative-first.

Nissen, Thomas Elkjer. "Social Media, Strategic Narratives and STRATCOM." *The Three Swords Magazine*, no. 28 (May 2015): 45-49. http://www.jwc.nato.int/images/stories/threeswords/SOCIAL_MEDIA_STRATCOM.pdf

Salmoni, Barak A. and Paula Holmes-Eber. *Operational Culture for the Warfighter: Principles and Applications*. 2d ed. Quantico, VA: Marine Corps University Press, 2011.

Zalman, Amy. "Narrative as an Influence Factor in Information Operations." *IO Journal* 2, no. 3 (August 2010): 4–10. http://legacy.crows.org/images/stories/IOJ_V2_I3a.pdf?phpMyAdmin=8fb0f1471e1062f3cc758f323e70b775

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website: https://armypubs.army.mil/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

Index

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

ATP 3-13.1
04 Oct 2018

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Acting Administrative Assistant
to the Secretary of the Army
1827001

DISTRIBUTION:
Distributed in electronic media only (EMO).

This page intentionally left blank.

This page intentionally left blank.